LA RED OSCURA

EN LAS SOMBRAS DE INTERNET

El cibermiedo y la persecución de los delitos tecnológicos

EDUARDO CASAS HER

¿Qué es la web profunda (deep web) o red oscura (dark net)? ¿Hay que tenerles miedo? ¿Es, acaso, como pasear por los bajos fondos de una ciudad? ¿Hemos de cuidar nuestra confianza en la red?

No solemos pararnos a pensar cómo funciona un motor de búsqueda de Internet y, precisamente, en su manera de actuar se encuentra su punto débil: la araña. Por mucho que se esfuerce el robot, hay lugares a los que no es capaz de llegar porque no está diseñado para ello. Y de esa red oscura a la que no puede acceder solo es visible el uno por ciento, el resto está escondido, como si de un iceberg se tratara.

Negocios ilegales, tráfico de armas y de productos, muertes retransmitidas, pornografía infantil… conforman el lado negativo de Internet; un pozo sin fondo que se abre desde nuestras pantallas. El autor de este libro, miembro del Cuerpo Nacional de Policía, que lleva desde 2004 trabajando en la Unidad de Investigación Tecnológica (UIT), nos explica con notable claridad cómo persiguen sin tregua y sacan a la luz los delitos de ese universo desconocido de la red.

Lectulandia

Eduardo Casas Herrer

La red oscura

En las sombras de internet

ePub r1.0
XcUiDi 31.08.17

Título original: *La red oscura*
Eduardo Casas Herrer, 2017

Editor digital: XcUiDi
ePub base r1.2

A los investigadores tecnológicos de la Policía Nacional
de ahora y de ayer.

AGRADECIMIENTOS

Un libro como este no es posible sin la ayuda desinteresada de un montón de gente, algunas de las cuales no han querido que las nombre, en especial compañeros de profesión.

Tengo que agradecer a Cruz Morcillo, periodista y amiga desde hace ya tantos años, que pensase en mí cuando este proyecto apareció por las mentes de la editorial. Le debo mucho, porque sin ella nada de esto habría sido posible. También envío un abrazo a Dani Montero, periodista, por aconsejarme, acompañarme y guiarme en todo este proceso, que ha hecho sencillo algo que no lo era.

Y, por supuesto, a mis editoras, Ymelda Navajo y Mónica Liberman, de La Esfera de los Libros. Si Cruz y Dani les hablaron de mí, ellas decidieron confiar y darme esta oportunidad única. Además, han respetado con notable estoicismo mis plazos y mi lentitud al darle a la tecla y sin apenas mandar matones a mi casa a indicarme que tal vez debiera acelerar el ritmo.

Les debo unas cervezas a mis amigos Leticia Jiménez y Carlos Berbell, por su ayuda ante mis dudas generales sobre lo que representa un libro de divulgación.

Un inmenso abrazo a mi amigo Juan Luis Chulilla, antropólogo y socio de la empresa de etnografía industrial Online and Offline S. L., además de colega en el foro de Defensa *www.portierramaryaire.com*, por su asistencia en el capítulo 3, al ayudarme a comprender la complejidad de Oriente Medio.

Irene Izquierdo, amiga desde hace media vida y mi ingeniera química de cabecera, me enseñó muchas cosas sobre centrifugadoras y gases pesados.

El inspector Javier Sánchez me explicó varios detalles sobre los negocios ilegales de Internet y cómo los delincuentes son también vulnerables en TOR, no en vano su grupo de Seguridad Lógica de la UIT ha detenido a varios.

Javier Izquierdo, un viejo amigo y mi economista de cabecera, me dio unas cuantas lecciones sobre términos de su especialidad, con los que logré comprender lo suficiente sobre cómo funcionan las monedas virtuales y lo que es el mercado.

El inspector y amigo Daniel Zarza me echó un cable con las estafas, desde el *phishing* hasta el *pharming*, pasando por todas las variantes imaginables, y me explicó una mínima parte de su amplia experiencia de campo.

Lorenzo Martínez, uno de los mayores expertos en seguridad informática en España y cabeza visible de la empresa Securízame, amigo desde que nos encontramos en una reunión de blogueros a la que me habían enviado mis jefes para representar a la BIT, me ayudó mucho sobre su complicado mundo, en el que *hackers* y delincuentes comparten espacio y técnicas con las que un simple mortal no sabe ni cómo empezar.

Pero si a alguien hay que agradecer que este proyecto haya llegado a buen puerto es al inspector David Sanz, amigo íntimo desde que vivíamos en Zaragoza y parábamos por la librería SaGa. Me ha enseñado un montón sobre sicarios, medicinas

ilegales y suicidas, campos en los que trabajó con éxito durante años, consiguiendo resultados que sorprenden dados los medios disponibles entonces y que solo se podían compensar con mucho trabajo. Pero es que, además, se ha leído todos los capítulos, los ha corregido, me ha aconsejado y sugerido y ha sido la mano amiga cercana que nunca ha fallado. Gracias de corazón, David. Tú vales mucho.

Y no puedo cerrar el capítulo de agradecimientos sin mandarle un beso a Jéssica Camino, mi pareja, la que ha insistido cuando me veía procrastinar, la que empujaba cuando algún tema se me hacía espinoso o cuesta arriba, la que siempre confía en mí, no importa lo que ocurra. Te quiero, pequeña.

1

INTERNET PROFUNDA. ¿QUÉ DEMONIOS ES ESO?

Warren Bulmer es un hombre grande, de casi dos metros, pelirrojo, que luce una cuidada barba. Llega a su despacho y cruza un cartel que advierte: «A partir de este punto puede usted encontrar imágenes desagradables en los monitores». Saluda a sus colegas y a su jefe, Paul Gillespie. Tras los formulismos de rigor y dejar colgada la americana en una percha, se sienta ante su ordenador con cuidado de que la corbata no acabe sobre el teclado. Es febrero de 2005 y acaba de iniciar su jornada en la Sección de Explotación Sexual de Menores de la Policía de Toronto (Canadá). Hace unos días encontró online a un pedófilo y va a continuar hablando con él. Sabe que es un tipo muy metido en las cloacas de Internet y que tiene información valiosa, por lo que merece la pena continuar exprimiéndolo. Poco podía imaginar que aquel día recibiría una imagen que daría inicio al caso más importante de su carrera, un niño vestido con una camiseta a rayas que sostiene en sus manos un teclado Logitech para ordenador, un modelo que solo se vendió en España y que daría origen a la Operación Kova en la que se detuvo en nuestro país al peligroso Álvaro Iglesias, Nanysex, y a su banda, formada por el leridano Eduardo Sánchez, Todd, y el orensano José Gómez, Aza, especializados en el abuso sexual de bebés y que hoy se encuentran condenados a entre ocho y cuarenta y cuatro años de prisión. El cuarto miembro, el murciano Antonio Olmos, solo fue condenado a tres años al ser su única misión distribuir en Internet lo que los otros producían.

Sin embargo, mientras en España todos estos individuos eran detenidos por la Brigada de Investigación Tecnológica de la Policía Nacional, los esfuerzos de Warren Bulmer en Canadá no iban a servir para identificar a su involuntario confidente, porque lo había conocido y hablaban a través de un sistema que impedía, a priori, rastrear las conexiones, denominado Freenet, un recurso muy útil para aquellos que quieren ocultarse de la acción de la justicia, popular en aquella época, sobre todo entre terroristas y violadores de menores.

Nanysex, sin embargo, no tomaba tantas medidas de seguridad. Al menos no con la profusión y cuidado de su amigo canadiense, y ese fue uno de los muchos fallos que cometió y que llevaron a su arresto. Supo que algunas de sus secretas imágenes de bebés habían llegado al gran público y empezó a volverse más precavido. Los investigadores llegaron a encontrar una nota en la que amenazaba a la persona que las había filtrado, porque se sabía «perseguido por el FBI».

Amplió su protección y empezó a enmascararse de una de las formas más habituales hace una década, recurriendo a las conexiones a Internet de otras

personas, en su caso, las de los clientes de la tienda de venta de ordenadores que había montado junto a su hermano y a los que acudía a configurarles el acceso a la Red. Esos eran los momentos que utilizaba para conectar sus cuentas, sabedor de que estaba a salvo de los rastreos de la policía. Con el tiempo y al ver que los agentes no llamaban a su puerta, volvió a confiarse y accedió a sus correos desde su negocio, lo que facilitó la labor policial.

Hoy, Freenet sigue existiendo y se utiliza, pero los delincuentes, y también aquellas personas celosas de su intimidad, han migrado a sistemas más sofisticados, como la red TOR, cada vez más popular, más sencilla y ágil. Lugar para venta de drogas, de armas, ataques a páginas web, robo de tarjetas, espionaje industrial y militar… y también refugio de conspiranoicos y hasta el sitio en que se fraguó la Primavera Árabe y donde se ocultan los disidentes de los países sin libertad, desde Cuba hasta China.

INTERNET ES MÁS QUE GOOGLE

¿Qué es la web profunda (*deep web*) o red oscura (*dark net*)? ¿Son sinónimos? ¿Hay que tenerle miedo? ¿Es, acaso, el equivalente cibernético a pasear por los bajos fondos de una ciudad?

No, no lo es. Internet es una revolución en las comunicaciones como nunca el hombre ha visto, aunque no solo eso. Su influencia en la sociedad es tan fuerte, tan honda, que condiciona las relaciones interpersonales, la forma de entender la actualidad y hasta la manera de aprender. Ya no es tan importante *saber* como *saber encontrar*.

La forma más habitual de utilizar Internet hoy es abrir el navegador —Explorer, Opera, Chrome, Firefox, etc.— y teclear en la barra del buscador Google aquello que deseamos encontrar. Al instante, obtenemos cientos de miles de resultados y solo tenemos que seleccionar el que deseamos. Hace tan solo veinte años eso hubiera parecido magia; hoy lo tenemos tan interiorizado que nadie piensa cómo funciona esa pequeña —no tan pequeña— maravilla.

Google es una empresa, creada en 1997 por dos estadounidenses, Larry Page y Sergey Brin, cuyo primer y más famoso producto fue un *motor de búsqueda* de Internet, el mismo que seguimos utilizando hoy en día y que en 1998 desbancó al que entonces era el más empleado, Altavista, desaparecido en 2013. Pero por muchos resultados que nos entregue, Google no es Internet. Apenas rasca la superficie de lo que aloja la Red. Si aprendemos su funcionamiento, entenderemos el motivo.

Google utiliza, en primer lugar, una herramienta llamada *crawler* —que se podría traducir por «reptador», aunque en español se ha popularizado como «araña»—. Este robot virtual —o *bot*— se dedica a recorrer la Red sin cesar, captando términos

relevantes, para lo que utiliza una serie de patrones informáticos conocidos como *algoritmo Google*. Todos los datos recogidos son después enviados a unos ordenadores que se encargan de *indexarlos*, esto es, darles una coherencia, buscarles unas correspondencias y ordenarlos de manera parecida al índice de un libro. Una vez generados esos índices, pasan por un tercer grupo de computadores que los clasifican según su importancia relativa, de manera que, cuando el usuario final —nosotros— teclee un término, le aparezcan en primer lugar aquellos más cercanos a lo que se desea encontrar según la lógica de las máquinas, que no siempre tiene que coincidir con la de las personas. Para esta tarea, Google dispone de instalaciones llamadas *centros de datos* por todo el mundo. Cada uno de ellos está formado por al menos treinta grupos de ordenadores y cada grupo lo componen entre cuarenta y ochenta equipos. La capacidad de almacenamiento estimada es al menos un millón de veces superior a la que tiene un usuario doméstico medio. Tengamos en cuenta que estos medios sirven tan solo para mantener los índices clasificados, no el contenido de las páginas, que están cada una en sus servidores y ninguno de ellos es Google. Eso nos puede dar un atisbo de lo titánico de su tarea.

En su manera de actuar está el punto débil de su funcionamiento, la *araña*. Por mucho que se esfuerce el robot, sus resultados van a ser siempre limitados y finitos, mientras que Internet se esparce de manera geométrica y hay lugares a los que el robot no es capaz de llegar. Algunos sitios le tienen vedada la entrada, como las redes que las empresas habilitan para que accedan sus empleados con un nombre de usuario y una contraseña que Google no tiene —ni debe tener—. Cualquier ciudadano o grupo puede tener una web privada impermeable a los buscadores.

En la actualidad, Internet se basa en las interacciones. Ya ha terminado la época en la que solo los expertos podían colgar su conocimiento en la Red. Dejando a un lado las redes sociales, una de las maneras más populares de llevar a cabo esta interacción es a través de *foros de Internet*. Son páginas web clasificadas por temáticas y, dentro de cada una, hay diferentes *hilos* en los que los participantes van escribiendo su aportación, que queda registrada en orden. A menudo estos foros tienen una parte pública, que todo el mundo puede leer, y otra privada, solo para los suscriptores —o para parte de ellos—. Los buscadores suelen estar vetados en esta última. En ocasiones ocultan toda una trama delictiva tras una pantalla de legalidad, como el sitio Los Nobles del Reino, desmantelado por la policía en 2009. Era un foro en apariencia dedicado a los juegos de fantasía épica, pero sus administradores mantenían oculta, no solo a Google sino al resto de usuarios, una auténtica red jerarquizada para producir y compartir pornografía de abusos a menores de la que no había ni la menor traza en la parte pública.

Claro que Internet no es solo la web, no es solo aquello a lo que podemos acceder desde el navegador. Es mucho más. Está llena de lugares a los que la araña ni siquiera puede llegar porque no está diseñada para eso; es como si pusiéramos una apisonadora a volar. No puede hacerlo. Entre esos lugares están, por ejemplo, el

correo electrónico, los servidores de archivos FTP, la mensajería instantánea (como Skype o el fenecido MSN Messenger) o su antecesor, el conocido chat.

IRC es el acrónimo de *Internet Relay Chat*, que se podría traducir por «charla interactiva en Internet». Es un protocolo de comunicación que existe desde 1988 y que se popularizó durante la primera década del siglo XXI. Aunque hoy en día se puede acceder a través de los navegadores —en parte gracias a que estos incluyen cada vez más capacidades y en parte por el esfuerzo de las empresas de IRC por dar acceso a sus servicios desde la web—, solo los programas dedicados permiten explotar todas sus posibilidades. En cualquier caso, incluso si utilizamos el Explorer, no estamos accediendo a la web y, por tanto, sus contenidos no son indexados… y no lo son porque no pueden serlo. Un chat consiste, a grandes rasgos, en un montón de personas comunicándose en tiempo real en una misma pantalla. Cada mensaje que escribe cada uno de ellos, por intrascendente o reiterativo que sea —y suelen serlo—, aparece en la ventana común y no queda registrado en ningún sitio. Como las palabras, se pierden con el viento, salvo que alguno de los presentes decida grabarlas.

Y, por supuesto, están los programas de intercambio de archivos entre iguales o *peer to peer*, utilizados de forma masiva para el tráfico de productos con derechos de autor como música o películas. Algunas estimaciones afirman que un ochenta por ciento de todo el tráfico de Internet lo acaparan este tipo de servicios que no aparecen en ningún buscador, más allá del que incluye el propio programa —cuando lo incluye — y circunscrito tan solo a su propia red.

Apenas hemos arañado la superficie nosotros también y ya podemos observar la magnitud de Internet y atisbar el significado de *deep web*, que proviene de la famosa *analogía del iceberg*. Por las leyes de la física, una de esas islas de hielo capaces de hundir barcos apenas asoma por encima de la superficie una séptima parte de su volumen total. De la Internet profunda se estima que el porcentaje visible es apenas del uno por ciento. La inmensa mayoría de ese noventa y nueve restante es accesible sin restricción alguna. Tan solo tenemos que saber cómo hacerlo (es decir, la dirección exacta).

El término *dark net*, red oscura, aunque en muchas ocasiones se usa como sinónimo (igual que Internet invisible, o Internet oculta, por poner solo un par de ejemplos más), tiene una etimología que puede interpretarse como más tétrica: aquello que está escondido, a menudo por ilícito, si bien otra tendencia entiende tan solo que no está «iluminada» por la luz de Google.

A la vista de lo explicado, pues, queda claro que la inmensa cantidad de Internet que no nos muestra Google no es mala por necesidad ni esconde delitos. Por otra parte, muchos delitos se gestan y ocurren en la Internet conocida —basta poner determinados términos en un buscador para encontrar horrorosa pornografía infantil, por ejemplo—. No hay, por tanto, que tenerle miedo *per se* a lo desconocido. Por supuesto, a veces sí que hay una parte que busca y desea la oscuridad. Y la ha habido desde que existe Internet.

El logro de la descentralización

Hasta el desarrollo de Internet, las redes de ordenadores eran algo muy diferente a lo que hoy conocemos. Un equipo muy potente, denominado *servidor* era el único *inteligente* y a él se enganchaban varios *terminales* que no tenían capacidad por sí mismos, sino que utilizaban la de aquel, tanto la de proceso (los cálculos a realizar) como la de almacenamiento (los documentos a guardar). También se entendía por red la conexión de dos o más ordenadores iguales entre sí, a través de determinados cables. Todas estas redes estaban en lugares relativamente pequeños, como el edificio de una empresa o un campus universitario. Es lo que hoy se conoce como «red de área local» y que muchas personas tienen en sus domicilios, a menudo sin saberlo, como cuando conectan portátiles, teléfonos móviles y tabletas a través del mismo *router*.

El problema de esas redes primitivas es obvio, son muy vulnerables. Si el ordenador central falla, toda la estructura deja de funcionar. En una época —los años sesenta— en que el mundo vivía atemorizado por una guerra nuclear, resultaba fundamental encontrar alguna manera de que los sistemas continuasen operativas cuando algunos de ellos se hubieran volatilizado en un hongo radiactivo. Ese fue uno de los motivos, pero no el único. El principal objetivo tenía un origen universitario. Todos los expertos querían tener los mejores ordenadores, lo que representaba una pérdida de dinero y esfuerzo si no iban a explotar todas sus capacidades. Era más práctico que cada universidad tuviera el mejor en un campo y las demás enlazasen con él, lo que además tenía la inmensa ventaja para profesores y alumnos de poder leer y consultar al instante a sus colegas de sitios lejanos sin la molestia de una llamada telefónica inoportuna o la exasperante lentitud de las cartas. La otra importante razón era la poca fiabilidad de las conexiones —relés— en aquellos tiempos. Cuando una fallase se necesitaba poder utilizar otra al instante sin que toda la red colapsara. Que el fallo fuese o no debido a un ataque con misiles intercontinentales era accesorio.

Hacía falta conectar computadores que estaban a mucha distancia. En vez de construir toda una nueva infraestructura, a dos estadounidenses, Leonard Kleinrock y Lawrence Roberts, se les ocurrió en 1961 utilizar una amplia red que ya existía por todo el país, bien trazada y muy ramificada, la telefónica. Cuatro años después consiguieron el hito de vincular de forma temporal un ordenador en Massachusetts con otro en California. Las señales viajaron por el hilo de cobre ya existente, destinado entonces solo a la voz, de punta a punta del país, cuatro mil ochocientos kilómetros. Así nació el concepto de «red de área amplia».

Después de un periodo de tiempo similar, a las 22.30 horas del 29 de octubre de 1969 se estableció el germen de Internet —entonces llamado ARPANET por las siglas en inglés de Red del Organismo para Proyectos de Investigación Avanzada— entre el Instituto de Investigación de Stanford y la Universidad de California en Los

Ángeles, a través de una más modesta distancia de quinientos ochenta kilómetros. Aquel primer enlace fue muy breve. Desde el segundo de los destinos pulsaron la letra L, que apareció al instante en el monitor del otro sitio. A continuación hicieron lo mismo con la O. Al intentar enviar el tercer carácter, la G, el sistema «se colgó». Todos los grandes caminos empiezan con un pequeño paso. El primer vuelo de un avión con motor de la historia, el de los hermanos Wright, duró solo doce segundos. Hoy, gigantescas moles de metal cruzan los cielos a velocidades impensables hace cien años. En 1971 ya eran veintitrés los ordenadores que formaban parte de la trama. Ese mismo año se envió el primer correo electrónico.

¿Cómo se comunican entre sí? Si un español y un ruso se juntan en una misma habitación y cada uno habla en su propio idioma, la comprensión será muy difícil o imposible. Si los dos han estudiado inglés, quizá utilizándolo puedan intercambiar información. Algo parecido pasa en una red. Todos los ordenadores, continuando la analogía, deben ser capaces de *hablar* el mismo idioma, aunque luego lo *traduzcan* a su *lengua natal*. En 1983 ese estándar se empezó a llamar TCP/IP, es decir «Protocolo de Control de Transferencias/Protocolo de Internet» por su significado en inglés. Fue una forma muy ingeniosa de reforzar el principal objetivo de Internet, una red descentralizada a prueba de fallos.

Cuando un ordenador quiere enviar un archivo (un texto, una foto, lo que sea) a otro en Internet, necesita hacerlo de una manera que logre que los datos lleguen a su objetivo. En vez de mandarlo todo de una vez, lo parte en pequeños trozos, llamados «paquetes». Cada uno contiene información sobre el lugar del que procede, al que se dirige y el puesto que ocupa en el conjunto de los paquetes enviados (para poder reconstruir el mensaje completo y con sentido) y, por supuesto, el trocito de datos que le corresponde. Estos paquetes son lanzados a Internet y cada uno recorre uno de muchos caminos posibles hasta que llega a su destino. Si alguno se pierde (por una *colisión* o por cualquier otro motivo), el receptor envía de manera automática una solicitud para que le reenvíen el trozo que falta y espera su recepción, todo ello en unos tiempos brevísimos. El movimiento de los paquetes por la Red no atiende a ningún orden preestablecido, solo buscan una manera de llegar a su destino. Por tanto, en caso de que alguno de los puntos por los que pasa estuviera fuera de servicio, elegiría otro que funcionase y el archivo llegaría de todas formas. Un sistema que puede parecer lento y farragoso pero es muy seguro. Como hemos dicho, a prueba de fallos.

Veamos un ejemplo simplificado. Queremos consultar la página web de nuestra editorial favorita —La Esfera de los Libros— en un ordenador. Para ello abrimos el navegador y tecleamos su dirección, *www.esferalibros.com*. Nuestro equipo envía unos paquetes que dicen: «¡Eh! ¡La Esfera de los Libros! ¡Quiero que me envíes tu página de inicio!». La máquina donde está alojada, llamada servidor, responde a la solicitud. Fracciona todo el contenido de la web en la cantidad de paquetes necesarios —a efectos de este ejemplo vamos a decir que son veinte, cuando en realidad serán

cientos o miles— y los envía a quien se los ha solicitado. En casa vamos recibiendo los paquetes y los vamos montando en orden, si bien, debido a la naturaleza del funcionamiento de Internet, han llegado primero los últimos y luego los del principio (cada uno puede elegir un camino diferente, recordemos, que no depende más que de la lógica de las máquinas). Sin embargo, el número 18 nunca llega y nuestro ordenador, que se encuentra que tiene el 17, el 19 y el 20, que viene marcado como «último», vuelve a contactar con la web de La Esfera para pedirle que le reenvíe lo que le falta. Todo ha ocurrido en breves segundos (o menos, dependiendo de nuestra velocidad de conexión) y lo único que nosotros, como usuarios finales, hemos visto es que en el navegador ha aparecido la página que deseábamos ver.

Internet es inmenso, lleno de millones de sitios web y de equipos informáticos solicitando contenidos. Entonces, ¿cómo sabe cada uno de ellos dónde debe dirigirse? Ya hemos visto que solo para los índices, Google utiliza almacenes de datos gigantescos.

La respuesta se llama *dirección IP*. Cada elemento que esté conectado a Internet, sea nuestro teléfono móvil o la web de la Policía Nacional, tiene asignada una de estas direcciones. Es la única manera de estar en Internet. Si no hay dirección IP, no hay conexión. ¿Acaso podríamos llamar al teléfono de alguien que no tiene número de abonado? Esto es similar, con una salvedad, aquellas pueden cambiar en muy poco tiempo y, de hecho, la mayoría de las conexiones domésticas lo hace.

Los ordenadores, en realidad, solo son capaces de llevarnos a direcciones IP. Cuando escribimos *www.policia.es* en realidad estamos acudiendo a unos dígitos escritos como 195.55.116.75. Cualquiera puede hacer esa prueba tan sencilla en su domicilio y observar los resultados: teclear en el navegador esas cifras y ver qué ocurre. Por tanto, «alguien» tiene que saber los nombres a los que equivalen todas esas direcciones, los conocidos como DNS o Servidores de Nombres de Dominio por sus siglas en inglés. Nuestro proveedor de servicios de Internet (Telefónica, Ono, Jazztel, etc.) nos configura sus propios DNS sin que tengamos que hacer nada más. Existen muchos otros. Google, sin ir más lejos, tiene los suyos. Consisten, en esencia, en una larguísima lista en la que a cada dirección IP corresponde el nombre de una web. Se actualizan cada poco tiempo, de manera que podamos seguir accediendo a los lugares deseados. Además, nuestro ordenador guarda una pequeña copia de las IP que corresponden a las páginas más habituales a las que solemos acceder, para ahorrar tiempo al no tener que hacer la consulta fuera del disco duro.

Los usuarios domésticos no solemos tener un nombre contratado, así que solo se nos «conoce» por nuestra IP que, como decíamos, puede cambiar con el tiempo. Si apagamos el aparato que nos conecta a Internet —hoy en casi todos los casos uno llamado *router*—, al volverlo a encender tendremos otra. Se debe a que las empresas a las que contratamos el servicio, y que son las que administran nuestras direcciones, tienen más clientes que direcciones para asignar, que son finitas. La actual versión (la cuatro) «solo» permite algo más de cuatro mil millones de direccionamientos. Pueden

parecer muchos, pero ya están agotados. Las últimas disponibles se asignaron el 3 de febrero de 2011 y, desde entonces, solo queda buscar la mejor manera posible de repartir las que hay. Esto se solucionará con la llegada de la nueva versión (la seis), que permite trescientos cuarenta sextillones. Esa cifra, que es difícil de comprender para los que no somos matemáticos, equivale a poner seiscientos setenta mil billones de IP en cada centímetro cuadrado de la Tierra. Impresionante, ¿verdad? Esperemos que no nos volvamos a quedar cortos en un futuro cercano…

De momento seguimos con la versión cuatro. Por eso, las compañías que dan servicio de Internet tienen que repartir lo mejor posible sus recursos. Saben que siempre hay un porcentaje de sus clientes que está *offline* (cuando acceden más clientes domésticos están apagadas cierto número de pequeñas empresas, por ejemplo) por lo que va asignando las direcciones disponibles entre sus usuarios a medida que estos las requieren y, cuando uno apaga su conexión, de inmediato esa IP que ha quedado disponible pasa a ser utilizada por otra persona que esté intentando acceder. Es lo que se conoce como *dirección dinámica* como contraposición de la *dirección estática,* que es la utilizada por las páginas web y algunos usuarios que eligen pagar más para tener una para ellos solos.

Por eso, para identificar a quien ha cometido un delito a través de Internet no es suficiente con la dirección IP, sino que hace falta, además, saber la fecha y la hora en que se cometió el hecho. Por supuesto, el mayor interés del delincuente es ocultar su IP, uno de los motivos por los que existen para ello redes específicas dentro de la *deep web*.

EL DELITO EN INTERNET. UNA PERSPECTIVA HISTÓRICA

El delito es inherente a la sociedad y los ordenadores no son sino una extensión de esta. Por tanto, las ilegalidades están presentes en ellos de la misma manera que en los demás aspectos de la vida cotidiana. Los delincuentes suelen actuar donde la ratio beneficio/riesgo es alta. Los años alrededor del cambio de milenio fueron un buen momento para ellos, puesto que la presencia policial era escasa. En la actualidad, aunque cada vez hay más agentes formados combatiéndolos, la Red sigue siendo un lugar muy apetecible, porque tienen varios elementos a su favor:

A. *Seguridad personal*: es menos arriesgado que atracar bancos o vender droga en la calle, incluso si te detienen.
B. *Ingenuidad del ciudadano*: una enorme cantidad de usuarios no tiene la formación mínima necesaria para tener unos hábitos de navegación seguros.
C. *Pluralidad de víctimas*: la enorme cantidad de usuarios —miles de millones— y el poco coste de la acción criminal sirve para obtener resultados óptimos con un porcentaje de éxito inferior al uno por mil.
D. *Transnacionalidad*: las legislaciones afectan a un solo país, mientras que la

actividad delictiva carece de restricciones; puede implicar una organización rusa que roba en España utilizando servidores ubicados en China y blanqueando el dinero en Marruecos y Brasil. Para algunos delitos, la colaboración internacional solo puede tener lugar si se supera una determinada cifra, por ejemplo de tres mil euros para algunos fraudes. Robando a cada víctima una cantidad menor, se aseguran una impunidad casi absoluta.

E. *Diferentes legislaciones*: los delincuentes aprovechan los vacíos legales de algunos países para ubicarse allí —como en el pasado ciertas islas del Pacífico que alojaban servidores con pornografía infantil porque sus leyes no lo ilegalizaban— o bien estados fallidos o en descomposición: muchos servicios de las redes ocultas se alojaban en Somalilandia, una zona semi-independiente de Somalia.

Casi cualquier delito puede tener lugar en Internet. Incluso asesinatos. Basta con que algún malintencionado cambie el programa que regula la medicación que ha de administrarse a un paciente ingresado en algún hospital, por ejemplo. Las ilegalidades tradicionales se adaptaron con rapidez a la Red. Las estafas, bien sean al ciudadano o al banco, solo cambiaron la forma de actuación; en vez del timo del tocomocho —la red criminal convence a un incauto de que compre un billete premiado de lotería que en realidad no es tal— se ha pasado al de las cartas nigerianas —nos escribe un príncipe africano que desea entregarnos su presunta fortuna (que no existe en realidad), para lo cual solo debemos enviarle dinero para «trámites administrativos»—. A partir de mediados de los noventa se convirtieron en un problema serio. Un informe del FBI de 1997 estimaba que los timos cometidos con tarjeta de crédito habían pasado a costar, en todo el mundo, de ciento diez millones de dólares en 1980 a mil seiscientos millones en 1995. Y lo peor estaba por llegar, dado que a finales del decenio comenzó la explosión de las mafias organizadas.

Otros hechos solo podían ocurrir dentro de una red, como la implantación de los programas malignos que conocemos como virus, gusanos o *troyanos* —*malware* es el nombre genérico—, destinados a replicarse, extenderse o controlar otro ordenador. El primero de estos molestos *bichos* fue creado en 1971. Se llamaba *Creeper* —Enredadera— y circuló sin problemas por ARPANET (el antecesor de Internet) sin que nadie pudiera detenerlo hasta que se creó el primer antivirus de la Historia, *Reaper* —Segadora—, destinado en exclusiva a su eliminación. El diseñador de aquel, Bob Thomas, tan solo quería comprobar si existía la posibilidad de que un programa se moviese y se autorreplicase entre ordenadores, pero la criatura se le escapó de las manos.

Durante mucho tiempo, estos virus no fueron más que una molestia o un programa muy malintencionado que causaba desde la destrucción de algunos o todos los datos del disco duro a la aparición de unas molestas barras verticales o que las letras que aparecían en la pantalla se cayesen a la parte inferior de la pantalla, como

afectadas por la gravedad. Hoy, toda esa inocencia ya no existe. El *malware* actual está diseñado por mafias organizadas con el propósito de obtener nuestros datos bancarios u otros elementos que puedan ser de su interés, o bien para crear la mayor destrucción posible en un sistema informático determinado. Su presencia es tan abundante y tan peligrosa que navegar sin un buen antivirus y un cortafuegos es poco menos que suicida. La pregunta en tal caso no es si vamos a tener un disgusto, sino cuándo. Por poner un ejemplo práctico, en una investigación llevada a cabo por la Brigada de Investigación Tecnológica en 2007, un individuo había intentado más de mil intrusiones en otros tantos ordenadores y solo había tenido éxito en aquellos que no tenían las protecciones referidas. En aquel entonces conocíamos a un «experto en informática» que aseguraba no necesitar esas defensas porque «con unos hábitos de navegación seguros no hay virus que acceda». Le convencimos para que analizara su ordenador para ver si estaba en lo cierto… y el antivirus encontró más de doscientas amenazas. Desde ese día es un converso. Lo que preocupa son aquellos que siguen confiando en su *ojo de buen cubero* para detectar los ataques y los que no han recibido la mínima formación imprescindible.

En la época de Internet, los delincuentes no necesitan verse jamás las caras. A menudo ni siquiera saben el nombre de sus compinches. Lo que hace falta es un lugar virtual de reunión para desarrollar sus estrategias, más fluido que el correo electrónico y más discreto que un foro público; un sitio para reunirse que esté fuera del alcance de las fuerzas de seguridad. Uno de los primeros fue el IRC, el sistema de chat del que hemos hablado más atrás.

Este servicio es como una pequeña Internet en sí mismo. Se organiza en servidores conectados entre sí para formar una red autónoma. Los usuarios acceden desde su domicilio a alguno de esos servidores y tienen acceso a todos los demás que utilicen la misma malla. Pongamos un ejemplo ficticio. Una red está formada por los servidores Alfa, Beta y Gamma. El internauta que acceda a Alfa puede hablar con cualquiera situado en los otros dos, ya que están enlazados. La única diferencia es el tiempo que tardarán en recibir su mensaje, que, salvo problemas, será algunas décimas de segundo más tarde que si estuvieran en el mismo.

Los lugares de charla, donde se juntan varios usuarios y todos pueden ver lo que otros comentan se llaman *canales*. Se crean y destruyen con facilidad y, por si eso fuera poco, se pueden declarar *secretos, de acceso solo con invitación* o *protegidos por contraseña*, para que, de esta forma, solo personas autorizadas por quienes los han creado puedan entrar. Si bien los grandes canales pueden estar monitorizados por los administradores, nadie controla lo que ocurre en esos pequeños lugares, salvo sus propios moderadores. Además, para mayor seguridad, los protocolos de IRC permiten que dos personas cualesquiera intercambien su dirección IP y, desde ese momento, mantengan una conversación directa en la que, además, pueden enviarse archivos, algo que no es posible en las zonas públicas. Como esas charlas e intercambios ocurren sin pasar por servidor alguno, son mucho más seguras.

Además de para los delincuentes que se coordinaban a través de estos chats para diseñar virus, estafas o realizar ataques informáticos, poco a poco fue popularizándose entre los menos avezados. No tardaron en aparecer canales dedicados al *warez*, esto es, el intercambio de material protegido por derechos de autor, desde música a *software*. Tuvieron su apogeo antes de que naciera Napster, el primer programa *peer-to-peer* (entre iguales), que permitía el intercambio de música que no estaba almacenada en ningún sistema centralizado, sino en los equipos personales de cada usuario. Pronto se programaron maneras automáticas de configurar el ordenador para que fuese un servidor de archivos (*Fserve* por su acrónimo inglés). Con estos *Fserves* se evitaba tener que estar aprobando manualmente cada envío o recepción. Bastaba con dejarlo encendido con ciertos parámetros —enviar un archivo por cada dos que se reciban, por ejemplo— para realizar el intercambio. Así pasaron de mano millones de canciones, películas en baja resolución y fotografías pornográficas. Era una época, finales de los noventa, donde las conexiones lentas no permitían los envíos de *gigabytes* de información.

En aquel tiempo los *activistas* se dedicaban a esta actividad poco legal en el mejor de los casos por altruismo. No ganaban nada por convertir las canciones al entonces nuevo formato llamado mp3 ni por enviarlas a terceros. Una red organizada, «Escena Mp3», que actuó desde mediados de los noventa hasta 2004 y pirateó un millón doscientas mil canciones, acabó por desaparecer debido, entre otros factores, a que los nuevos piratas quieren obtener un beneficio que ellos nunca buscaron. Habían quedado obsoletos.

Otros delincuentes no tardaron en descubrir el filón. Los pedófilos se instalaron con fuerza en IRC. Hasta mediada la primera década del milenio había canales dedicados con nombres tan explícitos como *#preteengirlsexpics*, esto es «fotos sexuales de niñas preadolescentes». La intensa presencia policial —solo en 2006 en España, la Operación Trigger de la Policía Nacional sirvió para detener a cuatro personas e informó a otros veintiocho países de un total de cincuenta y dos traficantes de imágenes de abusos de menores— consiguió que este tipo de delincuente cambiase el lugar de sus actividades. Los menos avezados migraron hacia las redes P2P (como eMule) mientras los expertos se introducían en lugares oscuros de la *deep web* como la red TOR. Si bien IRC era un lugar bastante privado, la necesidad de intercambiar direcciones IP para poder enviar y recibir fotos y vídeos tiraba por tierra toda seguridad.

El grueso de la cada vez más acusada actividad contra los derechos de autor pasó entonces a otro lugar de la *dark net*, las redes de intercambio *peer to peer* (o P2P), que se basan en que cada usuario individual decide poner a disposición de los demás miembros de la red, a los que no conoce, una serie de archivos que tiene en el disco duro y, a su vez, se descarga de otros como él lo que desea, cuyo único requisito es que también esté compartido. Así, cada día se generan millones de copias nuevas de música, películas, programas y libros.

El pionero, Napster, que ya hemos mencionado más arriba, pudo ser cerrado por las autoridades de Estados Unidos porque su estructura contradecía los principios de Internet. Tenía un servidor central que dirigía todo el tráfico. Una vez puesto fuera de servicio, la red dejó de existir.

Aquellos que tomaron el relevo no cometieron el mismo error. Ya no había un sitio que apagar. Tan solo con tener el programa adecuado (Ares, Gnutella, eDonkey…) no solo se accede a la red, sino que se es parte integrante de la misma. Algunas, las llamadas *híbridas* —por su necesidad de servidores además de usuarios finales interconectados— siguieron teniendo sitios que almacenaban parte de la información necesaria para que los demás se enlazasen entre sí, pero cualquiera podía convertirse en usuario o dejar de serlo sin que el conjunto se viera afectado. A todos los efectos era ya imposible de parar. Incluso si el programa original dejaba de estar disponible, los internautas creaban otros que utilizaban los mismos protocolos, es decir, accedían a la misma red, como el caso del que ha sido el medio más popular en España, la red eDonkey2000, creada en el año que su nombre indica. Fue desarrollada y mantenida por la empresa MetaMachine, de Estados Unidos, hasta que en 2006 llegó a un acuerdo con las entidades de gestión de derechos de aquel estado por el cual pagó treinta millones de dólares y cesaron sus actividades. Sin embargo, en 2002, un grupo de particulares, liderados por el alemán Hendrik Breitkreuz, habían creado su propio medio de utilización de esa red, el famoso eMule que todavía hoy continúa dando servicio a millones de personas en todo el mundo y que no se vio afectado por aquella resolución de la Corte Suprema del país americano. Siguen apareciendo nuevas versiones mejoradas cada poco tiempo, hasta treinta diferentes, como LPhant y aMule, que permiten dar servicio a ordenadores Apple Macintosh y sistemas operativos Linux. Cuando el número de servidores disminuyó, se desarrolló un sistema de conexiones directas que obviaba la necesidad de estos.

El motivo por el que muchos de los particulares que mantenían un servidor decidieron quitarlo después del 21 de febrero de 2006 fue la acción policial contra uno de ellos, Razorback2, alojado en Bélgica y cuyo titular residía en Suiza. A pesar de que no alojaba ningún contenido —tan solo ponía en contacto a gente que los tenía por medio de algoritmos, sin intervención humana— fue acusado de distribución de pornografía infantil, de difundir manuales terroristas, de fabricación de explosivos y violación de las leyes de protección de la propiedad intelectual e industrial. Sin embargo, la popularidad del sistema no decreció en absoluto y solo la llegada de sistemas más efectivos para intercambiar archivos hizo disminuir su tráfico.

Los P2P permiten saber la dirección IP de cada miembro de los mismos y eso los hace vulnerables. Solo en España se ha detenido desde 2005 hasta hoy a cientos de personas por utilizarlos para traficar con imágenes de menores explotados sexualmente. Todo lo que se hace en ellos deja un rastro detectable y rastreable hasta el origen. Esto se aplica también para otro tipo de ilegalidades que no entran en el ámbito penal. Que se lo cuenten a Jammie Thomas, una estadounidense condenada en

2007 a pagar más de doscientos mil dólares de compensación a la industria por haberse bajado veinticuatro canciones a través de estos sistemas entre iguales.

MOVERSE EN LAS SOMBRAS: DE LOS *PROXIES* A TOR

El problema con el que se encuentra aquel que tiene motivos para permanecer oculto es siempre el mismo, ¿cómo lograr que la dirección IP no sea conocida por la policía?

La primera solución es la más sencilla y la que menos conocimientos técnicos necesita. En vez de utilizar mi ordenador y mi conexión, voy a hacerlo con los de otra persona y, para ello, nada más fácil que acudir a un cibercafé o a un locutorio. Hace unos años eran muy populares, dado que una buena fracción de la población carecía de acceso a Internet personal y el inalámbrico gratuito que hoy se puede encontrar en casi cualquier establecimiento no existía. Tampoco llevaba todo el mundo un poderoso ordenador llamado «teléfono inteligente» en el bolsillo. Muchos ciudadanos y algunos delincuentes no tenían más opción que la de su cibercentro favorito, y así, cuando se realizase la investigación judicial, la única IP con la que se encontrarían sería con la del negocio, que en España no está obligado a guardar registro alguno de los clientes que usan sus servicios.

Este medio es efectivo si la actividad ilícita es ocasional y discreta, como un anónimo amenazante o un envío fraudulento. No es bueno para actos llamativos. Si alguien intercambia pornografía infantil en un sitio a la vista de otros clientes existe una buena posibilidad de que cualquiera, incluso el dueño, le denuncie. Si se intenta un ataque contra algún servidor, algo que requiere mucho ancho de banda, se va a notar. Con todo, algunas bandas comenzaron a operar todas las horas del día desde ellos. Uno de los casos más sonados ocurrió en 2005 en el ciberlocal Full Net, situado en la localidad de Almendralejo (Badajoz). Los delincuentes, una mafia con estructura y jerarquía, compuesta de veinte ciudadanos rumanos y un español, trabajaban de manera organizada, a turnos, durante las veinticuatro horas del día, realizando falsas subastas y ventas de las que se quedaban el importe que los incautos pagaban. Al utilizarlo como única «oficina», la Brigada de Investigación Tecnológica de la Policía Nacional pudo detectarlos, monitorizar su actividad —con la ayuda del administrador de la empresa, que nada tenía que ver con sus tejemanejes—, detenerlos y desmantelar la organización.

Descartada esa forma de ocultarse por vulnerable, el siguiente paso lógico es recurrir a otras conexiones de forma ilegal. Hasta mediada la primera década del siglo era necesaria una conexión física, lo que hacía el proceso complicado y poco práctico; muchos repararían en un cable colgando de su ventana. Aun así, se produjeron robos de información notables. Uno de los más acusados ocurrió en Estados Unidos en los noventa, cuando un grupo de *hackers* accedió en persona —es decir, acudieron al lugar con sus ordenadores— a la red de un hospital, que no era

parte de Internet, y consiguieron extraer los datos de miles de pacientes.

Durante aquella década se realizaron investigaciones fructíferas para eliminar el incómodo cableado. ¿No sería ideal que la señal viajase por el aire? Así podría conectarse un portátil desde cualquier lugar de la casa con mayor libertad y menos incordios físicos. En 1997 se estableció el primer protocolo funcional para permitir las conexiones inalámbricas —*WiFi*— y la primera norma, llamada 802.11b, data de abril del año 2000. No se popularizó en Europa debido a que utilizaba una banda de comunicaciones reservada a los militares. Tras muchos debates, con la versión «g», aprobada en 2003, se solucionaron los conflictos y los aparatos que daban ese tipo de servicio sustituyeron a los anteriores en poco tiempo. Hoy no es extraño que en una casa familiar entren a Internet una decena de dispositivos. Dos o tres ordenadores, un par de tablets, un teléfono por cada miembro de la familia y hasta la televisión… Todo sin llenar el suelo de engorrosos cables.

Durante los primeros años, estas nuevas conexiones no solían tener ninguna protección. Era habitual poder captar con un portátil las ondas y utilizarlas a conveniencia. Los delincuentes se movían en furgonetas que aparcaban delante de donde conseguían una buena señal, un lugar diferente cada día o cada pocas horas. Algunos preferían las zonas rurales porque, al ser casas bajas, el *router* estaba más cerca que en una ciudad, donde las emisiones de los pisos altos no llegan a la calle, y la vigilancia policial es menor.

Los proveedores de Internet avisaban de que el usuario debía activar los protocolos de seguridad, algo que era ignorado por muchos clientes que carecían de una mínima formación. Por ello, las empresas empezaron a enviar sus *routers* con estas medidas activadas, con la recomendación de que el cliente las cambiase por otras más seguras, porque las que se utilizan por defecto son conocidas de manera pública. Al principio eran todas la misma, dependiendo de cada compañía, y en la actualidad están asociadas al tipo de *router*. Es decir, existen unas listas consultables donde según el nombre asignado por defecto a la conexión, así será la contraseña. Cualquiera puede descargarse un programa para el teléfono que las contiene.

Incluso si el usuario las cambiaba por una de su cosecha, los primeros protocolos —llamados WEP por las siglas de Privacidad Equivalente a [conexión por] Cable, en inglés— eran vulnerables. Tenían ciertos fallos en la protección de la contraseña que hacían que unos ataques sencillos consiguieran averiguarla. La longitud de la misma solo servía para retrasar lo inevitable, el acceso del intruso. Las redes actuales implementan un sistema llamado WPA2 —Acceso Protegido *WiFi* por sus siglas en inglés— mucho más seguro, siempre que hayamos cambiado el *password* original y usemos uno de complejidad suficiente. Las mafias actuales utilizan potentes antenas —baratas de comprar en el mercado y fáciles de construir en casa— para buscar señales inalámbricas a muchos kilómetros de distancia. No necesitan realizar complicados ataques informáticos cuando pueden elegir de entre miles de personas aquellas que no se han tomado en serio su propia seguridad.

Una vez que el delincuente ha accedido a una *WiFi* la puede utilizar a su antojo. Es decir, todo el tráfico en Internet que realice aparecerá con la dirección IP del inocente ciudadano, que ni siquiera es consciente de lo que está ocurriendo. No solo eso, sino que todos los que están dentro de una red pueden observar con facilidad pasmosa lo que hacen los otros miembros de la misma —mediante un procedimiento que se llama de forma onomatopéyica *esnifar* y que consiste en capturar los paquetes que circulan por ella—. Es más, acceder a cada ordenador y consultar o adquirir los datos que contiene es sencillo. Han sido numerosos los detenidos en España por llevar a cabo ese tipo de robo de información. En 2013, en Zaragoza, se detuvo a un individuo que no solo accedía a las *WiFi* de sus vecinos, sino que activaba de manera remota la cámara web y grababa miles de imágenes de la actividad de estos. Ese mismo año se detuvo en Madrid a un joven de veinte años por utilizar la conexión de sus vecinos para conectarse a Internet. Los ejemplos son abundantes.

Del mismo modo, algunos expertos informáticos dejan intencionadamente abiertas sus conexiones para extraer datos de aquellos que las intentan utilizar. Así, el cazador se convierte en presa, a menudo sin ser consciente de ello.

Hay otros métodos para ocultar nuestra IP sin salir del domicilio y sin cometer ninguna ilegalidad *per se*. El primero de ellos y el más sencillo es el uso de un *proxy* —que podríamos traducir por «representante»— anónimo. Hemos explicado más arriba que, para solicitar una página web (por ejemplo *www.esferalibros.com*), nuestro ordenador envía un paquete con su propia dirección a la web donde está alojada aquella. De esta forma, *www.esferalibros.com* conoce nuestra IP y puede almacenarla en un *log*, un registro histórico de todos los requerimientos que ha tenido. Es decir, estamos localizados si alguien decide investigarnos. Un *proxy* es una máquina situada entre nuestro ordenador y el destino. En vez de solicitar la web de forma directa, nuestro ordenador contacta con otro al que le dice «¡Eh, *proxy*! ¿Puedes pedir La Esfera de los Libros y mandarme el resultado?». El aparato que recibe el encargo lo canaliza al servidor de nuestra editorial favorita y, cuando esta responde, nos lo envía de vuelta. En el registro de la web, la IP que queda almacenada es la de ese intermediario en vez de la nuestra. La Esfera de los Libros jamás sabrá para quién ha enviado sus datos. Creerá que lo ha hecho para alguien situado en Burundi, Indonesia, China o dondequiera que esté ubicado el proxy anónimo.

La idea original de estos *representantes* no es el anonimato. Tienen otra serie de funciones, como el filtrado de lo que puede o no entrar en un determinado espacio empresarial. Es habitual, por ejemplo, que las compañías bloqueen el acceso a páginas porno o de juegos de azar en la Internet corporativa. Los servicios de control parental, que evitan que los niños pequeños puedan acceder a contenidos inadecuados, también se configuran a través de ellos. En ocasiones, no obstante, pueden estar mal programados o configurados. En algunos casos, amantes de la privacidad los han dispuesto así a propósito. De manera excepcional, pueden ser una

trampa —llamada *honey pot*, tarro de miel— tendida por alguna organización gubernamental, sobre todo en países asiáticos como China o la ciudad semiautónoma de Hong Kong.

Existen listados públicos de *proxies* anónimos que se pueden consultar en Internet y se actualizan de continuo. Configurar un ordenador para utilizarlos es bastante sencillo con unos conocimientos mínimos. Hay incluso páginas web como *www.proxyanonimo.es* en las que no hay que hacer nada más que teclear en un cuadro de texto la web que queremos descargar a través de su intermediación.

El riesgo de estas herramientas, como comentábamos más arriba, es que no sabemos quién está detrás de cada una. Igual que una web suele mantener un *log* de los requerimientos que recibe, uno de estos servidores de representación puede hacer lo mismo, guardar la información de quién realiza cada solicitud y en qué consiste esta. Por tanto, podemos pensar que estamos haciendo una consulta anónima cuando, en realidad, estamos tan controlados como si no los hubiéramos usado.

El siguiente paso, por tanto, es complicar un poco más el juego de los *proxies*. En vez de uno, vamos a utilizar tres y que cada uno no tenga más información que la necesaria para hacer su solicitud. Esa es la idea que dio origen a la famosa red TOR.

El nombre que, salvo por una letra, recuerda al nórdico dios del trueno, es el acrónimo, en inglés de El Encaminamiento Cebolla (*The Onion Router*). La palabra «encaminamiento» o «enrutamiento» hace referencia al camino que va a seguir la información que pedimos y la que nos envían, desde que sale de nuestro ordenador hasta que llega al destino y vuelve de nuevo a nosotros. «Cebolla» es un símil sobre la forma en que se va protegiendo la identidad del que usa la red, poniendo una capa tras otra, como si fuera el culinario bulbo.

El sistema es muy fácil de utilizar. Tan solo debemos bajarnos un programa adecuado, el Navegador TOR —*TOR Browser* en inglés— que podemos encontrar en la propia web de la organización sin ánimo de lucro que gestiona el proyecto, *www.torproject.org*. Una vez instalado, basta teclear la dirección que queremos obtener y nos la hará llegar a través de un camino más seguro que cualquiera de los vistos hasta ahora.

Cuando realizamos una solicitud a TOR lo primero que hace es cifrarla, de forma que solo nosotros y el primer nodo al que conectemos conozca la petición. El citado nodo al que conectamos (que funciona como los *proxies* que hemos explicado) coge la información cifrada, incluyendo nuestra IP, y en vez de solicitar los datos al servidor, lo que hace es enviarle todo a un segundo nodo, que solo sabe que tiene una información encriptada y de qué máquina le ha venido, que, a su vez, también tiene su dirección camuflada mediante un algoritmo que solo conocen estos dos puntos intermedios. El segundo nodo tampoco hace una petición al servidor, sino que lo cubre con la «capa» de su identidad oculta y lo manda a un tercero que es quien, por fin, conecta a la Internet abierta y la única dirección IP que va a ser conocida por el sitio al que se han solicitado los datos.

Cuando empiezan a entrar los paquetes con la respuesta al nodo que los ha solicitado, este retira la capa que les había añadido y los manda al intermedio, el cual también quita la suya y los envía al primero, que realiza la misma función y nos los hace llegar. Así, tras tres pasos de ida, cada uno con una piel de cebolla más, y tres de vuelta, en que se va retirando cada una de ellas, podemos observar los datos de manera más o menos segura.

Cualquiera puede convertirse en un nodo, basta con disponer de una IP estática, un ordenador con suficiente potencia y un buen ancho de banda. Eso quiere decir que muchos están creados y monitorizados por agencias gubernamentales con el propósito de descubrir el tráfico que circula por ellos… pero para ello necesitan controlar los tres puntos de salto y eso, dada la inmensa cantidad de nodos que existen en una amplia pluralidad de países repartidos por todo el mundo, es muy complicado.

Resulta curioso que esté financiada, al menos en parte, por el gobierno de Estados Unidos, que es, a la vez, quien dedica más esfuerzos a acabar con el anonimato que proporciona. Fue anunciada en 2002 y empezó a funcionar al año siguiente, patrocinada y mantenida por el Laboratorio de Investigación Naval, un organismo que pertenece a la Armada de los Estados Unidos. En 2005 pasó a la entidad sin ánimo de lucro que la gestiona hoy. Según se puede consultar dentro de la propia web del proyecto TOR, que mantiene un registro constante de los accesos, el número de usuarios se mantuvo por debajo del millón hasta finales de 2013, cuando se disparó de golpe hasta quintuplicar esa cifra, si bien parece que tan notable subida se debió a que un alto número de ordenadores infectados por un virus llamado *Mevade* empezaron a utilizar esta malla para comunicarse entre sí. Desde entonces ha ido decayendo paulatinamente y en la actualidad se mantiene en torno a los dos millones.

La seguridad que ofrece no es absoluta. Como informa el propio Proyecto TOR, existen protocolos que pueden hacer que todo el esfuerzo de enrutamiento no sirva de nada. Las famosas *cookies* —pequeños ficheros de texto que las webs envían a nuestro ordenador— o el uso de extensiones que aumentan las capacidades de los navegadores, como Flash o Java, necesarios para ver de forma correcta muchos rincones de Internet, pueden ser utilizados para obtener la verdadera IP del requirente. Incluso puede sufrir ataques intencionados. Durante el primer semestre de 2014, una cantidad de nodos maliciosos pudo llegar a obtener datos fiables de hasta el ochenta por ciento de los usuarios, hasta que fueron descubiertos y eliminados a finales de julio.

TOR es más que un anonimizador, más que un *proxy* muy complejo. También permite mantener servicios ocultos (*hidden services*, en inglés). Existen páginas web situadas dentro de la red y a las cuales solo se puede acceder desde ella; no es posible desde ningún otro sitio. Se las reconoce por dos cosas, tienen el sufijo .onion (igual que las páginas españolas son *.es* o las comerciales *.com*) y su «nombre» es un código alfanumérico difícil de memorizar. Nada de términos sencillos como *www.policia.es*

o *www.esferalibros.com*. Todos deben contener exactamente 16 caracteres, comprendidos entre el 2 y el 7 y las letras «A» hasta la «Z», y no dependen de la voluntad del que las crea, sino que son una clave de seguridad encriptada, que impide saber qué dirección IP se esconde detrás de cada una de ellas. Por ejemplo, existe una copia de seguridad de la famosa WikiLeaks, de Julian Assange, a la que se puede acceder tecleando *http://zbnnr7qzaxlk5tms.onion/*. No existe ninguna autoridad que coordine ni almacene todos estos nombres, por lo que pueden existir sitios que jamás sean conocidos por el público, puesto que tampoco hay nada similar a un buscador. Lo más parecido son páginas como *The Hidden Wiki*, que se podría traducir como «la wikipedia oculta» o el *Directorio TOR en Español*, visitable en la dirección *http://cjxbupyxay3ibikr.onion/*. La vida de estos lugares es bastante breve. Algunos desaparecen y otros cambian su nombre cada poco tiempo. Por eso son importantes esos compendios, que son actualizados por los propios usuarios —nada de *arañas* rastreadoras, índices, algoritmos, etc.— a medida que los descubren o detectan su desconexión.

No solo se alojan páginas web. El sistema también permite correo electrónico y chats, entre otras cosas, que funcionan dentro del intrincado mundo de nodos y capas de cebolla.

Algunas personas consideran que la *darknet* la forman tan solo los servicios ocultos de TOR. Ya hemos aprendido que eso no es así. Muchos de los sitios más sórdidos y denigrantes están ahí, pero ni son los únicos ni siquiera los peores.

Antes de que existiera TOR, hubo, desde marzo del año 2000, otra forma en que las personas celosas de su intimidad se ponían en contacto entre sí, Freenet, ese lugar donde Warren Bulmer encontró la pista que le llevó a *Nanysex*.

Nació en 1999 como el proyecto de fin de carrera de Ian Clarke, un estudiante de la Universidad de Edimburgo (Reino Unido) y hasta el año 2002 no comenzó a utilizarse de forma organizada. Está en continuo desarrollo y cada poco tiempo salen actualizaciones que pueden descargarse de la página matriz, *http://freenetproject.org*. Su uso es muy sencillo, al menos para los poseedores de un PC estándar. Según sus propios datos, desde su creación han tenido dos millones de descargas. Sin embargo, algunas estimaciones cifran sus usuarios regulares en poco más de veinte mil personas, apenas una diminuta fracción de TOR.

Está basado en una premisa diferente. Cada miembro de la red habilita un espacio de su disco duro para que el sistema almacene en él contenidos, pero no sabe cuáles van a ser ni los tiene enteros. Por si eso fuera poco, además, los trozos que guarda están encriptados con una clave de alta seguridad. Es decir, estamos ante una red *peer to peer* como las que hemos explicado más atrás. Todo miembro de Freenet tiene el mismo nivel de jerarquía. No hay servidores que tengan las páginas web, sino que su contenido se reparte, en pequeñas porciones, entre cada uno de sus miembros. Cuando alguien hace una solicitud, el sistema busca los ordenadores que contienen los trozos deseados y los recompone poco a poco en el equipo del solicitante hasta

mostrar el documento completo. Las peticiones no son directas, sino que se realizan una serie de saltos entre quienes están conectados, de manera que no solo no se puede saber de dónde ha llegado cada porción —recordemos que las personas que lo almacenan no saben lo que almacenan—, sino tampoco el camino que han seguido. Dado que los equipos entran y salen de forma continua de Freenet —alguien accede, obtiene lo que desea y se va hasta que necesita algo más—, es necesario que no haya una sola copia de cada contenido, sino que se replique en una multitud de máquinas. De lo contrario, cuando alguien se fuese del sistema, ya no se podría acceder hasta que volviera.

En Freenet hay blogs, mensajes personales, foros y otros muchos recursos. Su apariencia es bastante diferente a una red P2P tradicional como eMule, por ejemplo, pero el funcionamiento interior es parecido, basado en la ausencia de servidores a los que hacer solicitudes y obtener respuestas. La principal pregunta que un posible interesado en Freenet debe hacerse es ¿estoy dispuesto a ceder una parte de mi disco duro para que alguien almacene en él pornografía infantil, mensajes entre terroristas o bienes robados? Nadie podrá acusarte de ello, puesto que no es tu intención tenerlo ni tienes los mensajes enteros, es tan solo una decisión ética.

¿Por qué hay tan pocos usuarios, entonces? Suele hacerse un símil con la carretera. Puedes elegir entre velocidad y seguridad. Si aumentas la segunda, a menudo vas a disminuir la primera y Freenet, por su propia naturaleza —no hay grandes máquinas conectadas, sino que la mayoría son ordenadores personales con conexiones domésticas— es lento. Muy lento. Tanto que puede desesperar a todos salvo a los más exigentes que, a menudo, son los delincuentes más recalcitrantes, los que más cuidado ponen en no ser detectados. TOR tampoco llega a una velocidad que hoy en día se considere aceptable y descargar archivos grandes —como vídeos, por ejemplo— puede llevar más tiempo del que estemos dispuestos a invertir en ello. Por si eso fuera poco, hay ciertas páginas de Internet que bloquean el tráfico que provenga de IP conocidas de la *darknet*, por lo que quien quiera descargarse algo debe hacerlo de manera pública o renunciar a ello.

Existen otros sistemas similares, como I2P (Proyecto de Internet Invisible, por sus siglas en inglés), que tiene unos treinta y cinco mil clientes, o nuestro caso español, Manolito P2P y Blubster, su sucesor, programas para compartir archivos desarrollados por Pablo Soto Bravo, que protegen la identidad de sus miembros. Debido a esto fue demandado en 2008 por las principales empresas del mundo audiovisual, Emi, Warner, Universal y Sony, que le reclamaban hasta trece millones de euros. En 2014, la Audiencia Provincial de Madrid le absolvió de todos los cargos y falló que no se puede hacer responsable al creador de una tecnología por el uso que se le dé. Tras esa sentencia, la última versión de Blubster puede ser descargada con total libertad.

El anonimato total, lejos de alcanzarse

Incluso los lugares de Internet más protegidos no garantizan un total anonimato de sus usuarios. No solo se pueden encontrar vulnerabilidades en los programas que se usan o inyectar nodos, como en la red TOR, para obtener auténticas IP, también existe la posibilidad de no tener bien configurado el ordenador y que esté suministrando nuestros propios datos sin que nos demos cuenta.

Además, por supuesto, está la información que entregamos de manera descuidada. Los delincuentes, como todos, cometen errores que les cuestan caro; pueden haber hablado de la ciudad en la que se encuentran o el sitio donde trabajan, subir una foto que lleva incorporados datos GPS o en la que se ve un lugar geográfico característico. La policía estará esperando el error que antes o después llegará.

Ciertos delitos también dejan un rastro palpable, el económico. Es muy difícil estimar el dinero que se mueve en la *deep web*, como lo es el de la economía sumergida de cualquier país. Solo a una página, si bien de las más importantes, *The Silk Road* —La Ruta de la Seda, en español, en la que se venden bienes ilegales, sobre todo drogas— se le calculó un movimiento de un millón doscientos mil dólares mensuales entre noviembre de 2013 y junio de 2014, que dejó unas comisiones a sus administradores, bajo el mando de Ross William Ulbricht, de noventa y cinco mil dólares por mes hasta su detención aquel año.

La Internet oculta incluso tiene sus propias monedas fuera del control gubernamental. Una de las más famosas es la Bitcoin, cuyo valor está asociado al tiempo de cálculo de los ordenadores y no a un patrón-oro o equivalencia similar y de la que hablaremos más adelante.

Aquí estamos ante la vieja dicotomía de la flecha y el escudo. Cuanto más fuerte sea la defensa que se desarrolle, más poderosa será el arma para vulnerarla. Es una carrera tecnológica que a veces ganará un elemento y a veces el otro.

El delito, no obstante, siempre va por delante, por una sencilla razón, hasta que no existe un método para delinquir no se puede luchar contra él. La policía se debe esforzar para ir tan solo un paso por detrás y no dos, gracias a su formación continua y al esfuerzo dedicado.

2

EL HOGAR DEL PEDERASTA

Holger Jaques es alemán. Es un tipo alto, con el cabello rubio oscuro. A veces se deja el pelo largo y una barba que no le favorece en absoluto. Un policía español, bajito y más bien grueso, lo está introduciendo esposado en un vehículo policial sin que pueda recoger a sus hijos en un colegio de Palma de Mallorca. Es el último día de clase antes de las vacaciones de Semana Santa del año 2011, unas fiestas durante las que pensaba violarlos, como hacía de forma regular cada vez que las reglas del divorcio le permitían quedarse a solas con ellos. Debido a sus antecedentes en Alemania por estafa y a su descuidado modo de ganarse la vida en España, tenía dudas de cuál había sido la razón por la que le habían leído los derechos. Después de todo, tampoco hablaba demasiado bien español.

Porque Jaques tiene un gran secreto, es el peligroso pederasta conocido como Cooldaddy (Papá Guay, en honor a la canción del grupo Boney M). No solo ha cometido abusos sobre sus hijos, sino también sobre los de sus parejas sentimentales, cuatro en total. A la manera del profesor Humbert de la Lolita de Vladimir Navokov, estaba en proceso de seducir a una nueva mujer, madre de una niñita de nueve años a la que pretendía llevarse a la cama. Más tarde, en los calabozos de la Jefatura Superior de la Policía Nacional reflexiona. No entiende cómo le han atrapado. Ha sido siempre cuidadoso en extremo. Está descartado que sus víctimas se hayan chivado, dada la manipulación que ejerce sobre ellos. Además, parece que los policías están empeñados en entrevistarlos. Si ya tuvieran sus declaraciones, no estarían tan pesados con ese tema, ¿no?

En Internet ha tomado siempre las medidas más extraordinarias para evitar su detección. De acuerdo, ha publicado en The Love Zone, uno de los foros especializados en pornografía infantil de la red TOR, varias de sus grabaciones teniendo relaciones sexuales, sobre todo con su hijita de cuatro años y también, aunque menos, con los otros tres. A su hijo, de siete, no. A él no le ha puesto nunca una mano encima. Solo ha hecho que penetre a su propia hermana de nueve. En sus vídeos editó con sumo cuidado todos los fotogramas en los que se podía ver su cara. El barco en que los grabó carecía de elemento personal alguno. El vídeo de presentación tenía unos carteles al principio en los que presentaba a los pequeños, pero a todos con nombres falsos. También incluía una dirección de correo para que otros pederastas contactasen con él. Solo había accedido a ella utilizando proxies, jamás en abierto. Tenía todos los contenidos de sus ordenadores encriptados con claves de alta seguridad. Sabía que ningún investigador lograría romperlas. Las tarjetas de memoria de las cámaras de vídeo las borraba cada vez que las copiaba. Eso limitaba mucho las cosas de las que le podían acusar. ¡No se veía su faz en

ningún vídeo! ¡Siempre podría decir que lo había hecho otro! ¡Pronto acabaría esa pesadilla!

Se equivocaba. Dos años después, desarmado de toda posible defensa por la abrumadora cantidad de pruebas que aportó la Brigada de Investigación Tecnológica, aceptaba una pena de diecisiete años de prisión y perder toda posibilidad de volver a ver a los chavales con tal de evitar un juicio público en el que sabía que iba a ser más expuesto aún a los medios de comunicación. Ya lo estaba pasando bastante mal en la cárcel como para que más presos supieran cuál era el motivo de su estancia tras las rejas.

LA CURIOSIDAD MATÓ AL GATO

Entre los legos en la materia existe la creencia de que la pornografía infantil consiste, sobre todo, en chicas adolescentes que se desnudan delante de un espejo o que son retratadas en poses «artísticas» y que luego, de una manera u otra, acaban en Internet. Esa no es la realidad. Al menos no toda. Ni siquiera es una fracción importante y, como veremos más adelante, quienes hacen eso suelen estar obligados o amenazados.

Los organismos internacionales aconsejan describir esta tipología delictiva con un término más cercano a la realidad, *explotación sexual de menores*. Lo que buscan los consumidores se divide en dos grandes áreas: *softcore* —desnudos— y *hardcore* —actos sexuales—. Chicos y chicas son víctimas por igual y el rango de edad va desde los pocos meses hasta la pubertad. A partir del desarrollo de los caracteres sexuales secundarios, la tipología cambia y el delito suele ocurrir por engaño o falsa seducción en vez de por abuso de confianza o compra. Las aberraciones más retorcidas también tienen su sitio, desde zoofilia a coprofilia, siempre con un pequeño en el centro de la «acción». Los autores en la gran mayoría de las ocasiones son personas muy cercanas a la víctima. Padres, familiares, tutores, profesores… Hay un porcentaje en el que el dinero está implicado. Suelen ser turistas sexuales occidentales en países del Sudeste Asiático, en especial Tailandia y Filipinas. Por otro lado, hay ciertas «empresas» del Este de Europa, sobre todo rusas y ucranianas, que pagan a madres por realizar fotografías *softcore* de sus vástagos. Es la excepción en un delito en que el interés económico, aunque mueve millones, no deja de ser una anécdota.

La legislación sobre la pornografía de menores es una de las más duras que tiene todo el código penal español. Hasta junio de 2015 estaba penada con un máximo de nueve años de cárcel la producción, distribución, donación, exhibición o cualquier muestra a terceros de ese material. En ese artículo se considera delictivo, al contrario que en la difusión de obras protegidas por derechos de autor, incluso enviar a otras personas enlaces donde se puedan ver esas imágenes. También está perseguido su almacenamiento en el propio disco duro o en «la nube» y, desde julio de ese año, incluso la visualización habitual puede llevar a quien lo haga a prisión. Por ello, en

este capítulo vamos a tener un cuidado exquisito en no proporcionar las direcciones donde se intercambian, muchas de las cuales están vigiladas por las policías de diferentes países. Recomiendo de forma activa que ningún lector busque estos contenidos, ni siquiera por ver de primera mano lo que contamos en estas líneas. Se está jugando algo más que un susto.

Este grado de persecución es superior a cualquier otro en nuestro ordenamiento jurídico. Ni siquiera en el caso de las drogas está penada su tenencia —aunque sí castigada por vía administrativa, como las multas de tráfico o las ordenanzas de ruido nocturno—. En años recientes, la ley ha evolucionado hacia un mayor reproche. Hasta la reforma del año 2003, la posesión era impune y hoy ni siquiera está permitido consultar una de esas webs con asiduidad. Esta dureza sigue los consejos de la Unión Europea, que incluso recomienda penar los dibujos animados o cómics con esta temática. En muchos países avanzados, sobre todo anglosajones, esto ya es así y está por ver cómo se interpreta la nueva redacción del artículo 189 del Código Penal, ya que parece que también van por ahí los tiros.

El activismo pedófilo considera por tradición que el consumo de ese tipo de imágenes no hace daño a nadie, puesto que por verlo no se está agrediendo a ningún niño y, por tanto, no existe victimización. Lo hecho, hecho está y que alguien tenga o no fotografías o vídeos no va a cambiar lo que ocurrió. La realidad rompe sus esquemas con mayor rapidez de lo que tardan en desarrollarlos. Cada persona, por supuesto, es diferente y hay excepciones a la norma, pero pongámonos en situación. Imaginemos por un momento, tanto hombres como mujeres, que nos han violado. Siendo adultos, que tenemos la mente más formada y se nos supone una mayor entereza que a un infante. No contentos con eso, han grabado los hechos y los han colgado en Internet y, como todo lo que entra en Internet, va a estar allí *para siempre*. Las personas que se descargan ese vídeo no lo hacen con propósito de denuncia social —ya sería malo que el mundo entero viera cómo nos violan—, sino *para satisfacer su deseo sexual*. Se masturban con él porque desearían hacernos lo mismo. Esa es la certeza con la que se enfrenta un niño del que han abusado, con la agravante de que, en muchas ocasiones, el responsable ha sido su padre, la persona que más confianza y seguridad debería ofrecerle en todo el mundo, con amenazas veladas y jugando con la psique infantil: «Este es nuestro secreto», «si cuentas esto a alguien te llevarán a un reformatorio y nunca más me verás a mí ni a mamá», etc. Ha habido suicidios por este motivo. En un caso, la víctima dejó una nota en la que explicaba que podía vivir habiendo sido violada, pero no sabiendo que esos abusos estaban en Internet para siempre y que, con seguridad, alguno de sus compañeros de clase ya los había visto. La dura realidad es que, cada vez que alguien ve a un menor víctima de un abuso sexual, ese menor vuelve a sufrir.

Aunque ese motivo por sí mismo sería suficiente para prohibir el tráfico y tenencia, hay otro igual de preocupante, si no más: el consumo de pornografía infantil propicia el abuso. Por supuesto, no todo individuo que disfruta viendo esas imágenes

acabará pasando a la acción, aunque sí ocurre a la inversa, casi la totalidad de pederastas productores de imágenes de los últimos quince años se han masturbado antes con la explotación sexual de críos que han bajado de la Red.

Existe un modelo psicológico para explicarlo. Ante la aparición de pensamientos sexuales desajustados —sexo con niños— el intelecto se encuentra con una barrera impuesta, la del castigo social, que les hace desistir. Sin embargo, a través de la satisfacción —orgasmo conseguido al mirar pornografía infantil—, esos obstáculos disminuyen. Observan que otras personas lo hacen y que, en apariencia, no obtienen una inmediata reprimenda. Así, a través de la repetición, cada vez tiene menos miedo y empieza a fantasear sobre víctimas concretas. Encuentra un decidido apoyo en las comunidades pedófilas, sitios de Internet, de los que hablaremos más tarde, donde se reúnen estas personas y que no son ilegales *per se*. En España fue paradigmático el caso del portal Protégenos, cuyo nombre era una burla a la ONG Protégeles, que durante muchos años abanderó la protección a la infancia. En inglés, uno de los más importantes es Boychat, heredero de *Boylover.net*, que también fue desmantelado por Europol en 2010 y decenas de sus miembros fueron arrestados.

En esas páginas se dan consejos sobre cómo «seducir» a un menor, cómo enfrentar las fantasías sexuales desde una perspectiva positiva, o se cuentan historias que pueden ser reales —estremecedoras en muchas ocasiones— o simples cuentos. Nada que condene la ley… salvo en el caso de que los hechos narrados sean ciertos, como se ha constatado en diferentes casos que han sido los detonantes de su desaparición forzada. Hoy, en Boychat se pueden leer consejos sobre qué hacer si la policía encuentra el rastro de sus actividades o un seguimiento pormenorizado de todos aquellos casos en los que ha habido detenidos y han trascendido a la luz pública.

Así, pues, el futuro agresor ve reforzada sus intenciones por el consumo de pornografía infantil y por el espaldarazo de esas comunidades. Las barreras psicológicas han desaparecido. Si tiene ocasión, actuará y lo hará sobre quien tenga más cerca. En nuestro entorno es muy extraño que ataquen a menores desconocidos, en especial en el caso de infantes. Ya pudimos ver lo que ocurrió con el pederasta de Ciudad Lineal, que despertó una alarma pública casi inmediata y una concienzuda *caza del hombre*. Las víctimas en casi todas las ocasiones van a ser cercanas, como familiares, amigos de la familia o aquellos que estén bajo la tutoría del autor. ¿Puede la prohibición de tener colecciones de niños violados repercutir en una menor incidencia de los abusos? Las teorías más importantes en Occidente van por ese camino. Son una mayoría los países de nuestro entorno que lo han prohibido y cada vez se unen más en América Latina.

Este es un delito que suscita un gran rechazo social. No solo está coordinada la acción policial, con la mayor parte de países trabajando al unísono, sino que los ciudadanos corren a denunciar en cuanto detectan el menor indicio. Grupos *hacktivistas* como Anonymous realizaron dos ataques, el primero en octubre de 2012

contra cuarenta sitios entre los que estaba la web Lolita City y el segundo en julio del año siguiente bajo el nombre *#OpPedoChat*. Su logro más significativo fue poner algunas de estas páginas fuera de servicio durante algún tiempo. También filtraron los supuestos nombres de los miembros de aquel foro, lo que nunca pudo ser verificado. En general, aparte de obtener notoriedad en los medios de comunicación, esas acciones carecen de cualquier validez o efecto a medio o largo plazo y pueden resultar perjudiciales, ya que ponen en alerta a los miembros y administradores de esos lugares y dificultan la acción policial.

EL *SEXTING* Y EL *GROOMING*: LA AUTOPRODUCCIÓN

La cantidad de pornografía infantil que existe es ingente y cada día aparecen nuevas imágenes. En el año 2014, un grupo de trabajo internacional analizó una *colección* que tenía un tamaño de más de cuatro *terabytes*. Un escueto doce por cierto era conocido. Peor aún, solo el cuatro por ciento mostraba a víctimas ya identificadas.

El esfuerzo policial en este aspecto es conjunto y coordinado. En Interpol hay un Grupo de Expertos en Identificación de Víctimas del que son miembros los países que disponen de especialistas en rescatar a chavales de esos abusos. Utilizan varias herramientas informáticas para dar a conocer a sus colegas del resto del mundo cada nuevo hecho que descubren y todos empiezan a trabajar de manera conjunta para tratar de saber dónde ha ocurrido. El resultado de sus pesquisas, así como todas las imágenes que han encontrado, es almacenado en una base de datos denominada ICSE DB —por las siglas en inglés de Base de Datos Internacional de Explotación Sexual de Niños—. Es una herramienta muy potente que permite comparar cualquier nueva fotografía o vídeo con los ya almacenados para ver si ya ha sido investigada o si es nueva. Y no solo eso, sus algoritmos detectan variaciones en la foto y estudian entornos y rostros, de manera que es capaz de determinar si lo que se ha analizado ha ocurrido en la misma habitación o si es el mismo menor en otro lugar.

Aquí, varios agentes del Cuerpo Nacional de Policía, adscritos a la Sección de Protección al Menor de la Unidad, forman parte de ese Grupo Internacional de Expertos.

Veamos un ejemplo práctico de cómo se trabaja. En una ocasión, Dinamarca encontró una serie de imágenes hechas dentro de un coche en el que se abusaba de una niña. En una de ellas se podía ver una botella de Mirinda. En España reconocieron una marca que los agentes pensaban extinta y que tan popular fue en décadas pasadas, así que investigaron quién la seguía fabricando y se pusieron en contacto con la empresa, PepsiCo, a la que mandaron un recorte de la imagen *saneada*, esto es, de la que se han retirado todos los elementos ilegales. En pocas horas, recibieron la respuesta que estaban buscando. Ese diseño en cuestión se fabricaba en Hungría y se vendía, además, en Rusia y Rumanía. Al final, fue en ese

último país donde se pudo ubicar a la chiquilla. Esto solo se puede hacer si se trabaja en común. De otra manera, la mayor parte de estos delitos quedarían impunes.

Hay que hacer una diferenciación entre la pederastia propiamente dicha y las imágenes autoproducidas por adolescentes que acaban en malas manos. Cuando hay un adulto o una diferencia de más de seis años entre la víctima menor de edad y el perpetrador, entra en el primer caso. Un niño no tiene voluntad sexual y cualquier acto de esa clase que se realice sobre él es delictivo de pleno derecho. Nuestro código penal es muy claro al respecto.

Por otra parte están las relaciones sexuales grabadas o las exhibiciones realizadas dentro de la relación normal de una pareja. En los adolescentes, que si no son *nativos digitales* cerca están de serlo y que desde pequeños han tenido una potente cámara en su bolsillo, es normal —y así hay que verlo— que, con el despertar de la sexualidad, hagan cosas que las generaciones pasadas no tenían a su alcance, por ejemplo, excitar a su chico o chica, que está en casa de sus propios padres, mediante la exposición del propio cuerpo. Esas imágenes las envían después a través del ordenador o de telefonía móvil. El problema con la pubertad es que es un periodo convulso. Un día los tortolitos se juran amor eterno y al siguiente se odian a muerte. Todos hemos pasado por esa etapa y lo sabemos. Una vez rota la relación existe la posibilidad de que uno de los dos decida *vengarse* de la otra parte haciendo pública la intimidad que tienen grabada. En esos momentos, aunque quien ha resultado expuesto se arrepiente y quizá no lo haga más, a menudo es demasiado tarde. Al contrario que en la pedofilia tradicional, este *sexting* va a tener un doble recorrido. Por un lado acabará en las manos de aquellos que se excitan con menores y, por otro, además, en todas las pantallas de compañeros, amigos, familiares y conocidos, con el brutal trauma que representa para el púber medio que su cuerpo y su sexualidad sean expuestos al cruel escrutinio de sus iguales. A menudo, esta segunda parte es peor que la primera, de la que quizá nunca tengan conocimiento.

Las leyes de la *viralización* no siempre están claras. Así, en la madrugada del 2 al 3 de abril de 2013 apareció en Internet uno de estos vídeos que en pocas horas se convirtió en *trending topic* en la red social Twitter, esto es, uno de los temas de los que más se hablaba en ese momento. Eso representa varios miles de *tuits* por minuto, muchos de los cuales llevaban incrustado el vídeo, que después de unas horas estaba en muchas páginas web de todo el mundo, además de una intensa distribución por WhatsApp, que tres años después todavía no ha acabado.

El hecho había ocurrido en el anterior verano. Una pandilla de adolescentes se encontraba en un aparcamiento cercano a la playa de su ciudad. Entre ellos estaba la novia de uno que, en un momento determinado, decidió realizar una felación a su chico delante de los demás, con la condición de que no lo grabaran… Absurdo pensar que al menos uno de los cinco quinceañeros con un teléfono en el bolsillo no iba a inmortalizar tan atolondrada conducta. Para colmo, mientras estaba metida en faena, un tercer chaval le apartaba el pelo de la cara para facilitar la tarea. De ahí el nombre

con que se popularizó, «el mamazo con palanquilla» con el *hashtag* —etiqueta dinámica que permite una búsqueda rápida— *#MamazoPalanquilla*.

Una vez almacenado permaneció en el anonimato del grupo de púberes hasta que el noviazgo acabó poco antes de la fatídica fecha. Entonces, el novio despechado, por venganza, lo distribuyó por el instituto en el que estudiaban, donde estuvo algunos días hasta que alguno de los cientos de chavales que lo tenían lo subió a Internet y se desató la locura. La involuntaria protagonista tuvo que eliminar su cuenta de Twitter y sufrió graves consecuencias psicológicas. Hubo una víctima colateral más, el *Palanquilla*, al cual la humillación también afectó de forma superlativa. Su último mensaje, antes de verse forzado a dejar la red social fue un doloroso «menuda me espera mañana en el instituto». Quien lo grabó y el exnovio frustrado que lo distribuyó fueron detenidos y acusados por la Fiscalía de Menores.

Aquella noche de principios de abril, los expertos de la Brigada de Investigación Tecnológica tuvieron que hacer horas extra, a menudo trabajando desde sus propios domicilios, para conseguir, con notable éxito, cortar la difusión pública de aquellas imágenes ilegales y así proteger, en la medida de lo posible, la privacidad e indemnidad sexual de los menores de edad. Claro que la policía no puede ni debe comprobar los teléfonos y ordenadores de cada español que se lo ha descargado, así que se sigue deteniendo hoy a gente que lo intercambia por mensajería telefónica. Y no, no son pederastas, pero están cometiendo un delito, como hemos explicado al principio de este capítulo.

El segundo origen de las imágenes ilegales proviene del *grooming*, una palabra de curioso origen —su significado original en inglés es cepillar las crines de un caballo— que define las técnicas destinadas a conseguir imágenes sexuales de un menor y, en última instancia —ese paso final no ocurre a menudo y el agresor se conforma con el previo—, abusar en persona de él. El *groomer* es un auténtico depredador y a menudo su crueldad es inaudita, superior a la de los pederastas en sentido estricto, que buscan racionalizar una conducta no violenta, al menos desde su particular punto de vista y excepción hecha de aquellos que tienen comportamientos sádicos.

El proceder de estos individuos es tan similar que en ocasiones cuesta distinguir a unos autores de otros. La policía tiene su perfil psicológico muy estudiado. Suelen ser muy activos y sus víctimas se cuentan por centenares o miles. Dado que su campo de acción es Internet, no tienen que limitarse a la cuidadosa «seducción» personal o al niño al que tengan acceso. En lugar de eso, lanzan el señuelo a cientos de incautos a la vez con dos estrategias iniciales, el ataque informático o social o la simpatía desde una personalidad inventada. Su actitud depende de si disponen o no de herramientas para amenazar desde el principio.

El acosador tipo tiene creados múltiples perfiles en las redes sociales que frecuentan los niños, Tuenti, Facebook, etc. En aquel lugar donde haya menores, allí estará. Usa fotos del chico o chica que atraiga al segmento de población al que desee atacar. Por ejemplo, en una investigación de la BIT, el autor, un muchacho gaditano,

se hacía pasar por *Elisa* o *Lisha*, la fingida hija del embajador español en Estonia, para así conseguir engañar a los que él buscaba, chicos jovencitos, rubios y de piel blanca.

Una vez en esa red, inicia búsquedas selectivas y va agregando a chavales. Es habitual que mande solicitudes a todos los miembros de un mismo colegio o centro social. Cuando le acepta el primero, los demás van haciéndolo con confianza, dado que ya es *amigo* de uno de ellos. Como los chavales hacen «carreras de popularidad» de forma habitual, con el objeto de conseguir la mayor cantidad de contactos, es bastante sencillo para estos delincuentes penetrar el círculo. Va hablando con ellos, conociéndolos, preguntándoles por sus gustos… De esa manera va a tener datos muy válidos que le pueden servir para adivinar la contraseña del pequeño y tomar el control de su perfil en Internet. Así, podrá suplantarlo y tener una cuenta más convincente que la suya, que está hecha con datos fingidos.

No tardará mucho en conducirles a una charla sexual. Al inicio de la adolescencia, la curiosidad impulsa a las víctimas a seguirle la corriente. Si ya rondan la quincena, aún inocentones, caerán en el juego de la falsa seducción. De verdad creen que están ante el chico o chica de sus sueños y no ante un tipo que puede tener veinticinco o sesenta años y que, desde luego, no se parece en nada a la foto que ha compartido.

Antes o después, el *groomer* tendrá algo con lo que iniciar el chantaje. Quizá ha conseguido una foto en la que la niña enseña los pechos o tal vez, con un programa diseñado para ello, ha grabado la emisión de la cámara web en que el niño muestra el pene. En ese caso, la amenaza de enviarlo a amigos, familiares y compañeros de colegio es suficiente. Quizá ha averiguado sus contraseñas y amenaza con hacerse pasar por la víctima y comportarse de forma promiscua. Aunque no tiene imágenes comprometidas, usará otras y el efecto será el mismo. O tal vez ha infectado con un troyano el ordenador o el teléfono del pequeño y tiene total control y conocimiento de lo que en ellos hay. Con ese recurso incluso puede activar la webcam y haberle grabado al ir o volver de la ducha o cuando se cambia de ropa por las mañanas. En cualquier caso, desde ese momento se quita la falsa careta de la amabilidad y descubre su lado cruel… una crueldad que puede llegar a costar vidas. El gaditano estuvo acusado hasta del suicidio de una de sus cerca de cincuenta víctimas, a la que indujo a usar la pistola del abuelo, presa de la desesperación.

Estos acosadores suelen poner plazos y cuotas a sus víctimas. El célebre *Camaleón*, el «ciberacosador de Chipiona», que fue condenado por el Supremo a ciento noventa y dos años de prisión, de los que solo cumplirá once, exigía a las chicas que le dedicasen todo el tiempo que considerase oportuno, incluyendo la mayor parte de las noches. Así, iban a clase sin apenas dormir, con el consiguiente bajón de rendimiento. A él, que no trabajaba ni estudiaba y se levantaba pasado el mediodía, le daba igual. Les exigía cuatro o cinco vídeos pornográficos a la semana y, si no cumplían, enviaba los que ya tenía a amigos y familiares. Como infectaba sus

ordenadores, sabía detalles íntimos que usaba para amenazarlas hasta el punto de que alguna de las chicas tenía miedo incluso de salir de casa. Habían dejado de acudir a clase y de hablar con sus amigos, debido al pánico. Todo eso sin llegar a ponerles un dedo encima. No es necesario para arruinar muchas vidas. En su caso, al menos ochenta y una se presentaron al juicio, de las más de doscientas cincuenta que localizó la Policía Nacional.

Otros autores, los menos, desean llegar al contacto físico. Fue el caso de la Operación Tamo. Manuel Joaquín Blanco García buscaba a chiquillas de doce años a las que «enamoraba» y esperaba a que cumpliesen los trece para tener relaciones sexuales con ellas, lo que hacían engañadas. Lo hizo en al menos dos ocasiones, aunque los intentos se contaban por miles. Si se resistían o querían terminar la «relación», la crueldad de sus acciones no conocía límite, llegando a causar trastornos alimentarios y depresiones severas. Un individuo de cincuenta años tiene conocimientos y experiencia vital más que suficiente para conducir a chiquillas de esa edad como quiera, más aún cuando lleva dedicadas miles de horas de su vida a aprender cómo hacerlo mejor y a buscar los potenciales objetivos, inabarcables.

En los servicios ocultos de la red TOR existen sitios web dedicados al tráfico de imágenes que proceden en exclusiva del *grooming*. Allí se reúnen acosadores sexuales de todo el mundo para poner en común sus *hazañas*. Entre ellos se felicitan y se dan respaldo psicológico. Su mayor recompensa —y la única— es el espaldarazo social en su reducido círculo.

Uno de esos tipos era Arturo Dodero Tello, un peruano que se hacía llamar *Maxi* cuando entraba a la web con mayor tráfico de delincuentes sexuales de habla española, Lolita City, hoy desmantelada e inactiva. Su forma de actuar, expansiva y cuidadosa, sembró de víctimas España e Iberoamérica. La Brigada de Investigación Tecnológica de la Policía Nacional tenía monitorizada la página en la que iban apareciendo, con preocupante regularidad, nuevas víctimas. A menudo lloraban e imploraban que las dejase en paz, con vacuo resultado y ante los aplausos de sus secuaces. En los textos que acompañaban a sus vídeos, afirmaba ser argentino, algo que no convencía a los investigadores. Su forma de escribir no era europea, pero tampoco parecía platense. Ver los vídeos, uno tras otro, y no poder hacer nada era tan frustrante como angustioso. Las niñas existían. Eran reales. Cada día había más. ¿Era imposible encontrar al autor? Dentro de TOR las IP van cifradas, ya lo sabemos. Esa vía quedaba descartada. Los investigadores empezaron a usar caminos alternativos. Tal vez si consiguieran identificar a alguien que apareciera en los vídeos… Así se pusieron a una de las tareas más exigentes para la psique de cualquier persona normal, y también de las más importantes en su trabajo, la identificación de víctimas. Procedieron a desmenuzar cada uno de los vídeos que *Maxi* iba subiendo, estudiando hasta el mínimo detalle. Había que encontrar algo que pudiera servir. Algún despiste. Algún error. Siempre los cometen. Este caso tenía la dificultad añadida de que del autor, como perpetraba sus crímenes detrás de una cámara web, no iba a aparecer

ningún elemento personal que lo señalase.

La suerte, como es habitual, sonríe a quien la busca. Una de las niñas aparecía vestida con un uniforme escolar en el que se veía, diminuto y borroso, el escudo del centro. Podía estar en cualquier lugar del mundo o la policía podría no ser capaz de descifrarlo. Su perseverancia les dio la recompensa. Era un colegio de Las Palmas de Gran Canaria. Tenían su rostro y sabían dónde estudiaba. Lo más complicado estaba hecho. Un equipo de la Brigada de Investigación Tecnológica se desplazó a las Islas Afortunadas y no tardaron en poder entrevistar a la pequeña y a sus padres, que, como es natural, dieron permiso para estudiar su ordenador. Entre los contactos de Skype de la niña estaba el correo utilizado por *Maxi*, según ella misma les indicó y pudieron corroborar. TOR es lento y con poco ancho de banda, quizá demasiado escueto para realizar videoconferencias. Había tenido que arriesgarse y utilizar una conexión abierta, fuera de la seguridad del enmascaramiento de IP. Sus accesos reales llevaban a Perú, lo que era consistente con las investigaciones previas.

El mismo equipo de profesionales de la BIT cogió un avión y aterrizó en Lima para coordinarse con la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional de aquel país, que prestó todo su apoyo y colaboración. Juntos, no tardaron en encontrar el domicilio que Dodero compartía con sus padres. Obtenido el permiso para el allanamiento del domicilio y acompañados de la fiscal peruana, se dispusieron a la ejecución de la diligencia. El sospechoso vio llegar a los agentes e intentó darse a la fuga. Fue interceptado antes de coger la suficiente distancia y conducido al interior del recinto. Los agentes españoles que asistían en calidad de invitados obtuvieron permiso para ayudar a sus homólogos a revisar el ordenador presente en el domicilio. Para su disgusto, no encontraron nada, más allá del programa que permitía acceder a TOR. Indicio marginal en el mejor de los casos. Existía la posibilidad de que no pudieran acusar de nada a uno de los tipos más malvados y crueles con los que se habían enfrentado. Uno de los agentes españoles, Pedro Romero, reparó en que uno de los puertos USB del equipo, por los que se podían conectar elementos de almacenamiento masivo como *pendrives* o discos duros extraíbles, estaba inmaculado, mientras que los demás presentaban una más que notable suciedad. Algo había estado *pinchado* ahí. Como el investigado no quería contestar, iniciaron una concienzuda revisión de toda la casa, centímetro a centímetro. ¡Tenían que encontrarlo!

Las horas pasaban sin que el dispositivo apareciese. Quizá lo había destruido antes de iniciar su abortada huida o tal vez lo había arrojado fuera de la vivienda, donde alguien podría habérselo llevado. Cuando ya parecía todo perdido, los policías tuvieron una sospecha. El padre no se había levantado del sitio en que se encontraba durante todo el tiempo, mientras que el resto de personas presentes en el domicilio se movían de un sitio a otro. Se le ordenó apartarse del sillón y, debajo, apareció un disco duro que poco tiempo llevaba allí. En él se encontraban todas las pruebas necesarias. *Maxi* había sido detenido y retirado de la circulación. Incluso sin poder

obtener los datos de la *deep web*, el anonimato total es una quimera cuando hay policías motivados tras cada delito.

ADULTOS QUE EXPLOTAN A NIÑOS

Con el *grooming* y el *sexting*, hasta ahora no habremos visto más allá del diez por ciento del total de pornografía infantil que se mueve en Internet. El resto está formado por los abusos de un adulto sobre un niño de corta edad, grabados por aquel, y por la explotación «comercial» de la infancia. Veamos esta última.

La tradición atribuye el origen de la pornografía infantil al diácono británico Charles Dodgson, conocido por el pseudónimo de Lewis Carroll, con el que publicó dos libros que forman parte de la historia de la literatura universal, *Las aventuras de Alicia en el País de las Maravillas* y *A través del espejo y lo que Alicia encontró allí*, sin duda marcados por la amistad que el religioso tenía con la niña Alice Liddell, cuyo crecimiento se ve reflejado en la tristeza que emana la segunda obra en comparación con la anterior. La mayoría de fotografías que realizó Dodgson, entre 1856 y 1880, de las que solo una tercera parte ha llegado a nuestros días, muestra a niñas pequeñas desnudas o semidesnudas. En realidad, ese tipo de fotos ya existían en la era victoriana, al igual que la prostitución infantil, a unas escalas que hoy serían impensables y cuyo reproche social era casi inexistente. El inmortal autor fue tan solo el primero al que se le pudo poner nombre y de ahí tan oscuro patronazgo.

Tenemos que dar un buen salto hacia delante en el tiempo para encontrarnos con la empresa danesa Color Climax Corporation, con sede en Copenhague. Durante diez años, desde 1969, produjo películas comerciales en las que se abusaba de niñas entre los siete y los once años, en ocasiones incluso más jóvenes. Los cortos duraban diez minutos y el título de la serie era, como no podía ser de otra manera, *Lolitas*. Se conservan al menos treinta y seis diferentes con títulos como *Pre-Teen Sex* (Sexo preadolescente) o *Sucking daddy* (Chupándosela a papá). Aprovecharon un vacío legal en Dinamarca —aquello que no está prohibido está permitido— para realizar su actividad hasta que la legislación les impelió a cambiar el objetivo de su pornografía, que llegó a ser de las más reputadas por su calidad, con revistas, ya con modelos adultos, como *Color Climax* o *Rodox*.

La llegada de Internet supuso una mayor facilidad para llegar al consumidor final, al pedófilo, que propició la aparición de empresas como Ukranian Angels Studio, conocida por el público como «LS Studio», activa entre 2001 y 2004, que llegó a explotar a más de mil quinientas niñas entre los ocho y los dieciséis años y a ingresar cientos de miles de euros en los tres años que duró su actividad. Esta empresa no mostraba abusos sexuales en sus fotos, sino tan solo desnudos, de ahí su sobrenombre «LS» por Lolitas Softcore. El siglo XXI no es 1970 y la pornografía de menores está castigada en casi todas partes, por lo que la policía ucraniana reventó sus actividades

y detuvo a sus responsables. Había miles de suscriptores a sus productos de todos los rincones del mundo.

Este delito no es patrimonio exclusivo del Este de Europa. La última operación se gestó en Canadá cuando la empresa Azov Films fue desmantelada por la Policía de Toronto en 2011. Su principal cabecilla, Brian Way, ha sido condenado por quince cargos en la Corte Superior de Justicia de Ontario. El resto de sus secuaces ya habían reconocido ser culpables de los hechos imputados para evitar el juicio público. Vendían, bajo el aspecto de la legalidad, vídeos de niños y adolescentes jugando y luchando desnudos, tratando así de bordear el límite del delito. Algunos de los vídeos podían ser categorizados como «inocente» nudismo, pero la mayoría de ellos, por el tratamiento que se daba a las imágenes y la fijación con los genitales de los pequeños entraba dentro del tipo penal y así lo entendieron no solo Canadá, sino Estados Unidos, Hong Kong, Sudáfrica, España, Alemania y Suecia, entre otros. Azov Films y sus filiales trabajaban bajo una falsa apariencia de legalidad, registrados como empresa y pagando impuestos por sus actividades. Además, tenían una serie de mensajes en su web que afirmaban que no se incumplía ninguna norma en sus productos, lo que atrajo a muchos pedófilos que se consideraban a salvo.

Después de que la Policía de Toronto cerrara la empresa y detuviese a los responsables, llegó el momento de buscar a los compradores, clientes que habían ido acudiendo de todo el mundo durante los cinco años de actividad que tuvo la mercantil. La persona que está dispuesta a pagar, más aún todavía con su propia tarjeta de crédito, por acceder a ese tipo de imágenes, está un paso más allá que el simple consumidor. Ha disminuido lo suficiente sus inhibiciones, como explicábamos antes, para ser un peligro social. Y así fue. Durante el transcurso de esa segunda fase de la operación se rescató a trescientos ochenta y seis niños que estaban siendo explotados por los clientes «para su propio disfrute», sin relación alguna con los «protagonistas» de las películas de Azov Films. En España la Policía Nacional detuvo a cuarenta individuos, de los que cuatro, además, abusaban de niños, en algunos casos incluso por la fuerza. Se identificaron veinte víctimas entre los diez y los catorce años.

De esta forma llegamos a la verdadera naturaleza de este delito, a la inmensa mayoría de la producción que se incrementa a diario con cientos de nuevos pequeños sometidos a abusos, el ánimo lúbrico. Hacer fortuna no es el propósito de la mayoría de productores de pornografía infantil. Se consume con su simple visionado y, cuando una escena se ha visto las suficientes veces, ya no provoca las mismas sensaciones; el adicto necesita buscar material nuevo.

Los archivos de abusos a menores se esparcen en tres círculos concéntricos. El más exterior es el primer sitio al que acude quien no tiene contactos, es decir, a Google o a otros buscadores de Internet y a las redes P2P, como eMule o Ares. Las estimaciones de Interpol afirman que el ochenta por ciento de todo el tráfico de abusos a menores se produce en esos lugares. No presentan una especial dificultad

para su rastreo, por lo que cada año son detenidas cientos de personas que se dedican a esa actividad, con el agravante de que, en la mayoría de las ocasiones, por la naturaleza de su funcionamiento, están distribuyendo a la vez que descargan, por lo que se enfrentan a penas mucho más graves que el mero poseedor. Lo que se encuentra en esos sitios no es nuevo. Se nutre de la producción industrial que ya hemos tratado, tanto reciente como antigua, y de lo que se filtra de los grupos secretos que se dedican a abusar de niños y compartir entre ellos sus abusos. Es lo que los expertos denominan *el tercer círculo* y está infiltrado con profusión por agencias policiales de todo el mundo. Cada vez que algo nuevo aparece en esos rincones en los que se mueven los menos duchos en ese mundillo es analizado con profusión por los expertos en identificación de víctimas para intentar rescatarlas.

Dentro de ese mismo tercer círculo están los foros públicos de la red TOR y de Freenet, esto es, aquellos donde no hace falta aportar nada para participar. En ellos, amparados en la falsa sensación de anonimato, gente como *Maxi* comparte sus atrocidades. Los más taimados se reservan para otros lugares donde se sienten más a salvo. A menudo, los productores —esto es, gente que abusa de niños y lo graba o les toma fotografías—, se relacionan solo entre ellos. Ese contacto puede ser de forma bilateral (a través de correos electrónicos o sistemas como Gigatribe) o bien en sitios web donde solo los que aportan violaciones recientes tienen acceso. Como saben que se están arriesgando a muchos años de cárcel, suelen tomar muchas medidas de seguridad. Es posible que no solo haya que enviar una foto de abusos que sea nueva, sino que en ella se vea un cartel con el apodo del usuario que la envía y el nombre del sitio al que quiera acceder (como, por ejemplo, *Hoarder's Hell*). Estos forman el denominado *primer círculo*, impermeable a la acción policial hasta que algún miembro del entramado cae. Entonces es hasta cierto punto fácil detener al resto. Para satisfacer sus ansias, han intercambiado entre sí los abusos que cada uno ha cometido sobre los niños que tienen a su disposición y, en ocasiones más datos, hasta números de teléfono. Dado que este es el único delito que consiste en grabar las pruebas del mismo, solo hay que asociar cada violación a los datos disponibles de cada agresor que pueda proporcionar, de forma voluntaria o no, el ya detenido. No hay que entender este círculo como único, sino que está formado por multitud de grupúsculos, asociados por sexo de las víctimas y grupo de edad. Los pederastas tienen claras sus preferencias: bebés, hasta los seis años, hasta los diez o hasta el desarrollo de la pubertad. Aquellos que tienen una elección concreta consideran que la suya es la correcta y que son aquellos que se excitan con más jóvenes los verdaderos pervertidos. Una vez desmantelada una banda, la caza continúa y el trabajo policial vuelve a empezar desde el principio.

¿Y el *segundo círculo*? Lo forman los amigos de los «productores». Son aquellos que no abusan —por falta de oportunidad o cobardía, aunque con el adecuado deseo de ello—, pero tienen la suficiente confianza con los que sí lo hacen como para que estos les envíen sus «obras». En principio es difícil de penetrar por las fuerzas de

seguridad, salvo que cometan un error. Son más proclives a ello, puesto que se juegan menos. No es comparable la pena por tener o distribuir a la que puede caer por abusar. Cuando metan la pata, que lo harán, puesto que, como humanos, no son infalibles, se podrá llegar de nuevo al primer círculo y conseguir el que es el principal objetivo de las policías del mundo en esta especialidad, rescatar a las víctimas, poner a salvo a niños que han sido sometidos a abusos, en ocasiones durante mucho tiempo, y cuyas experiencias tal vez les marquen la vida para siempre.

The Love Zone era uno de los foros sobre abusos a menores más activos que había en la red TOR hasta que desapareció en 2013. Sus creadores habían descubierto que eran víctimas de una vulnerabilidad que podía haber revelado la verdadera dirección IP de todos los que accedían a él, así que, tras colgar un cartel de aviso, los borraron en un intento de proteger a sus «clientes».

Dos años antes de eso, cuando el sitio aún era seguro, había tenido, entre otros «famosos», a Holger Jaques, miembro de un *primer círculo*, el tipo que no se explicaba cómo le habían atrapado a pesar de sus medidas de precaución. Su primer vídeo fue descubierto por la policía danesa. Era una especie de «tráiler» al estilo de los cinematográficos, que comenzaba con un mensaje en un inglés macarrónico. Se presentaba como *Cooldaddy* y hablaba de sus hijos, a los que se refería como Julia, de ocho años, Mike, de siete, y Lisa, con tan solo cuatro. Los nombres, es obvio, eran falsos; las edades no. Ofrecía intercambiarlos con otros pedófilos «como él», así como traficar con vídeos. Para ello ponía el correo que utilizaba en ese momento, *cooldaddy@emailn.de*, tras advertir que lo cambiaría en un par de meses para evitar el rastreo policial. Tras esas cortinillas, el resto de la duración de la *demo* consistía en los serios abusos cometidos por un adulto sobre un niño y dos niñas. Había todo tipo de atrocidades sexuales, que incluían penetraciones entre ellos y con el padre. El rostro de *Cooldaddy* quedaba siempre oculto, pero no así los grandes tatuajes que le cubrían todo el brazo derecho.

Como todos los presentes hablaban en alemán, Dinamarca remitió el vídeo a través del Grupo de Identificación de Víctimas a ese país, donde la Policía Federal comprobó que el acento les correspondía a ellos y no a otros lugares como Suiza o Austria. De inmediato pidieron las direcciones IP de acceso al *email* que había proporcionado, tan solo para encontrarse con una sucesión de *proxies* que enmascaraban la verdadera IP. El siguiente paso fue solicitar la interceptación de las comunicaciones. Así fueron leyendo cada uno de los mensajes que cruzaba con sus «admiradores» y obtuvieron algunos escasos datos. El único fiable fue que comentaba que el sitio para «intercambiar» menores era España, su lugar de residencia y donde en el pasado había regentado un club de tenis. De esta forma acabó en manos de la Brigada de Investigación Tecnológica de la Policía Nacional. Los expertos españoles se pusieron de inmediato a hacer lo único que se podía en este caso, desmenuzar hasta la saciedad el vídeo para obtener algún detalle, por nimio que fuese, que sirviese para llegar al objetivo.

Lo primero que llamó la atención era que estaba rodado en el amplio camarote de un barco, de forma más o menos circular y con una claraboya en el techo. La ausencia de objetos personales en las mesillas les condujo a pensar que tal vez no fuera de su propiedad, sino que lo tuviera alquilado o, más probablemente, que trabajase en él como mecánico. Eso lo dedujeron de las manos que, cuando se mostraban en pantalla, tenían alguna sustancia oscura bajo las cortas uñas, tal vez grasa. No eran manos delicadas. El individuo debía de dedicarse a algún trabajo manual y la reparación de yates le venía como anillo al dedo. Como en el interior de la península no hay demasiados mares, había que buscar por la costa. Otro detalle acotó más la búsqueda. En una de las escenas aparecía un fragmento de una gorra en la que se podía leer *ca'n*, es decir «casa de» en mallorquín, tal vez el nombre de un restaurante. Era suficiente. Un equipo se trasladó de inmediato a Palma, donde se coordinaron con la Brigada Provincial de Policía Judicial de la isla para rescatar con la máxima urgencia a las víctimas. Faltaban pocos días para la Semana Santa de 2011.

Montaron tres subgrupos. Uno iría por los colegios con las fotos de los niños, puesto que en alguno debían conocerlos; el segundo acudiría a todos los concesionarios de venta de yates para tratar de localizar el modelo exacto y el tercero buscaría por los talleres de reparación de embarcaciones, donde intentarían encontrar al violador.

El primer resultado positivo llegó de los vendedores de barcos: el camarote era el de un Rodman 56, uno de los modelos más comunes en nuestras costas. Ese camino iba a ser complicado. Los centros educativos tardaron dos días en dar resultados, cuando un centro para alemanes creyó reconocerlos y, tras algunas gestiones adicionales, al fin se consiguieron algunos apellidos. El problema era que ya no estudiaban allí y no aparecían empadronados en ningún lugar de las islas. Al menos ya tenían un nombre con el que trabajar, Holger Jaques, del que no tardaron en saber que tenía antecedentes en Alemania por estafador y en España había sido investigado en una operación contra la pornografía infantil del año 2007, aunque no se logró dar con él y escapó tras sufrir un registro en su empresa. Una búsqueda en Internet lo encontró como donante de semen y, a través de ese rastro, acabaron dando con otro buque, un velero llamado *SY-Berill*, que explotaba para los turistas junto a otro amigo. Eso podía explicar sus manos callosas y sucias, dado que ambos eran todo el equipo de mantenimiento. Una búsqueda nacional lo encontró anclado en el puerto de Málaga, en reparaciones. Ya no era de su propiedad. Los agentes de la Policía Nacional en la Costa del Sol realizaron un reportaje fotográfico que ratificó lo que ya se sabía, que no era el mismo camarote.

Las fiestas se acercaban y el nerviosismo de los investigadores, más. Si no lograban encontrar a los niños antes de las vacaciones, quedarían a merced del violador durante al menos otras dos semanas. Trabajando sábado y domingo, buceando hasta en el último documento oficial, consiguieron otro prometedor

resultado. El Boletín Oficial de las Islas Baleares hablaba de unas becas para dos niños apellidados Jaques que acudían a un colegio público de la capital. Aquel lunes hablaron con la directora, que reconoció a ambos. El círculo se cerraba. Esos niños siempre acudían con la madre. Del progenitor, separado, no sabían nada. Una vez más, la suerte sonríe a quien la busca. Al día siguiente la directora recibió una llamada telefónica porque el Miércoles Santo quien recogería a los chavales sería Holger. Así se pudo preparar su detención y evitar más sufrimiento a los más inocentes de toda esta historia.

El tema estaba claro. Tenían el tatuaje de su brazo, la gorra y otros elementos, que se encontraron en su chalet, y hasta juguetes sexuales que guardaba junto a los propios de los niños… pero todos sus ordenadores estaban encriptados. Parecía que no se podría recuperar nada hasta que una vez más la pericia y el buen hacer de la BIT consiguió el tesoro. En el coche que usaba encontraron una tarjeta de memoria que pertenecía a una cámara de vídeo. Estaba borrada, nada que un especialista no pueda recuperar. Comenzaron a aparecer multitud de vídeos que habían pasado por ella, casi todos ellos con los abusos sobre la más pequeñita de las chicas, de tan solo cuatro años. También se encontró el original, sin editar y sin cortinillas, del que se había grabado en el barco. Las pruebas en su contra eran abrumadoras. Las víctimas eran tanto sus hijos naturales como los de una de sus exparejas. En los correos intervenidos en Alemania hablaba de una mujer ciega a la que estaba seduciendo para abusar de la hija de esta, de siete años, de la que ya había programado el abuso.

Hoy, un lustro después, siguen apareciendo en diferentes lugares de Internet, muchos de ellos de TOR, nuevos vídeos con la explotación sexual de aquellos cuatro niños, de tan prolífica que fue su actividad antes de ser detenido. A pesar de sus medidas de precaución, a pesar de moverse solo con *proxies* y en la *deep web, Cooldaddy* también cayó. Como suelen decir los especialistas de la BIT, cuando hay niños en riesgo, no se repara en esfuerzos para rescatarlos. Lo único que lamentan es no poder haberlo hecho antes.

La Internet doméstica cada día tiene unas capacidades más asombrosas. Hoy es común mantener videoconferencias en alta definición de larga duración. Va arrinconando a las comunicaciones tradicionales, en especial desde el extranjero, donde resulta más barato utilizar la conexión inalámbrica del hotel que una conferencia internacional.

Esa oportunidad no ha tardado en ser aprovechada por una de las industrias que más abierta está a la innovación, por contraposición a sus primas ricas —cinematográfica y musical—, el porno. Los *grandes* estudios de la especialidad están siendo sustituidos por chicas, chicos o parejas *amateurs* que graban desde su domicilio y luego lo venden en páginas web montadas por ellos mismos. Una vuelta de tuerca más les ha llevado al *streaming*, esto es, el sexo en directo. Los actores o actrices realizan espectáculos utilizando sus cámaras web en páginas dedicadas a ello como Chaturbate, de una manera muy parecida a los locales de *strip-tease*

estadounidenses o a las cabinas de *sex-shop*. Durante el *show*, los espectadores, que se pueden contar por millares, realizan pequeños pagos voluntarios («propinas») a cambio de lograr un objetivo común (retirada de la ropa, penetración, orgasmo) que el actor realiza al llegar a una determinada cantidad económica. Además, por más dinero se puede solicitar un pase privado, la grabación de un vídeo o serie de fotografías.

Las redes de explotación de niños han copiado ese modo de actuar y las últimas tendencias van por ese camino. En el Sudeste Asiático y, en especial, en las Islas Filipinas, se han encontrado varias redes que explotan a niños de ambos sexos y de amplio rango de edad según los deseos de quien está al otro lado. Si bien no se han detectado amenazas a la vida de los pequeños, sí que se han plegado a los deseos de los clientes del resto del mundo, que incluyen hasta sacrificios animales en el proceso. El pago se debe efectuar de una manera que escape a los controles financieros, como en el resto de transacciones del mercado negro. Para ello estas tramas criminales utilizan dos opciones diferentes. La primera es el pago a través de entidades no rastreables, como Western Union. De esto hablaremos en profundidad más adelante, en el capítulo seis. La otra manera es pretender que se paga por otros servicios, como pornografía legal o por conceptos del todo diferentes, como instrucciones de programación o manuales de *software* que se realizan a través de plataformas de pago *online* como PayPal. Una vez que han cobrado, se lleva a cabo la exhibición utilizando servicios de videoconferencia muy conocidos, como Skype.

¿Qué nos deparará el futuro? Los delincuentes sexuales avanzan con la tecnología tan rápido como los nuevos sistemas aparecen. Hoy son las videollamadas, mañana algo que hoy todavía no ha sido inventado.

ACTIVISMO PEDÓFILO O CÓMO JUSTIFICAR LO INJUSTIFICABLE

La mayoría de personas que se excitan con niños son varones. Ese porcentaje aumenta más entre quieres recurren a la pornografía en todas sus escalas —tenencia, distribución y producción— para satisfacer esas necesidades. Esto es debido a que la excitación visual funciona mejor con los hombres que con las mujeres, las cuales prefieren textos escritos donde la imaginación juegue un mayor papel. En Internet existen muchas páginas dedicadas a los relatos eróticos. Suelen tener un apartado dedicado a historias sobre relaciones sexuales entre adultos y niños. Es fácil comprobar que el porcentaje de féminas presentes es alto, sobre todo en comparación con otras parafilias. Tan solo en aquellas relacionadas con la dominación y la sumisión suele haber más —lo que explica el éxito de novelas como *Cincuenta sombras de Grey*—. Lo cierto es que, hoy, la literatura erótica sobre menores no es delictiva, por explícita que sea, por lo que esa conducta es impune. No son del todo extrañas las noticias en las que una mujer ha iniciado una relación con un adolescente

que no está en la edad de consentimiento, como el caso, entre otros, de la estadounidense Katerina Bardos que, con veinticuatro años, mantuvo una larga relación sentimental que incluía sexo habitual con su alumno de doce, al que también suministraba marihuana, hasta que fue detenida a mediados de 2015. Es un caso paradigmático. La pedófila suele tener una sola víctima, al contrario que el varón, en el que es extraño que no abuse de varios niños, salvo que le resulte imposible el acceso a ellos.

No obstante, hay mujeres involucradas en la producción de pornografía infantil. El caso más habitual es aquel en el que se encuentran bajo la influencia de un varón dominante. Cuando están junto a él ocurren los abusos y, si la relación termina y dejan de verse, incluso aunque ella siga al cargo del menor, estos desaparecen como si nunca hubieran ocurrido. Está también el caso de la prostitución infantil que las madres alientan, estimulan o al menos permiten y no es raro ver en grabaciones realizadas en el Sudeste Asiático —Tailandia y Filipinas en la mayoría de ocasiones — a estas junto a sus vástagos. Este es un caso diferente, puesto que no estamos hablando de un verdadero deseo, sino de una suerte de relación laboral, por desnaturalizada y reprobable que nos parezca; por supuesto, ilegal y tan perseguible como aquella que se hace por deseo. El futuro de un niño violado nunca va a ser tan positivo como el que no lo ha sido, por uno u otro motivo. En España también han sido detenidas consumidoras y traficantes de estas imágenes, algunas declaradas pedófilas, como la dueña de un kiosco de Segovia que fue arrestada por la BIT. Son excepcionales, pero existen, en la misma medida en que la pornografía de adultos cada vez tiene más aceptación entre el público femenino, sobre todo las nuevas generaciones que ya han nacido con Internet, con todo el sexo del mundo a un clic de distancia.

El perfil del individuo envuelto en el tráfico de pornografía infantil es tan variado como impredecible. La mayoría son hombres —con las excepciones que hemos detallado— y pertenecen a todas las clases sociales, económicas y culturales. Aparte de eso, los hay solteros, casados, que comparten piso, con hijos —víctimas propiciatorias—, sin ellos, etc. En caso de los *productores*, se puede estrechar el círculo un poco más. Suelen buscar trabajos y dedicaciones relacionadas con la infancia como profesores, monitores de tiempo libre, animadores y cualquier otra donde puedan acceder a un infante.

El caso por antonomasia de este tipo de comportamiento es del Gabriel Jordá Correcher, que aceptó una condena de seis años de prisión por la Audiencia Provincial de Valencia por producir y distribuir pornografía de menores de trece años, con el agravante de ser su cuidador. Este individuo orientaba toda su actividad al contacto con niños. Estudiaba magisterio, realizaba prácticas en colegios, era payaso y animador cultural, organizaba campamentos de verano y daba clases particulares gratuitas. Aprovechaba toda situación en la que se quedaba a solas con sus alumnos para desnudarlos y azotarlos (práctica que se conoce por su nombre en inglés de

spanking). Grababa estos vídeos y los distribuía entre sus contactos, alguno de los cuales le ayudaba a modificarlos para que su rostro no fuese visible en Internet. Después de ser detenido por la Brigada de Investigación Tecnológica, ingresó en la prisión de Picassent algunos meses y, tras pagar una fianza, recuperó la libertad. Como no le habían retirado el pasaporte, escapó a Guatemala, donde fue encontrado de nuevo por la Policía Nacional… ¡en un orfanato!, desde el que pretendía evitar la acción de la Justicia española. Fue extraditado y, por fin, pudo ser juzgado y sentenciado en nuestro país.

Internet ha traído cosas buenas y malas al mismo tiempo en la lucha contra la explotación sexual de menores. La gran ventaja es algo que ya hemos mencionado más arriba. Desde que Internet es popular, los pederastas que antes cometían los abusos en la intimidad, ahora graban y comparten la prueba de su delito. De esta forma se puede rescatar a muchas víctimas que hasta los años noventa permanecían desconocidas, sufriendo sus horrores sin nadie que les pudiese ayudar. La otra cara de esto es la estigmatización de las propias víctimas, como ya hemos comentado también antes. Pero hay algo más: hasta entonces, los pederastas eran personas asociales, esquivas; no tenían posibilidades de hablar de su *afición* que, como no podía ser de otra manera, llevaban en secreto porque el reproche social y penal era muy grande. El pedófilo tipo era un señor que merodeaba por colegios y parques infantiles. Con la llegada de Internet, obtuvieron algo que, siendo legal, es terrible, la posibilidad de crear comunidades, de ponerse en contacto entre sí, de darse un *refuerzo positivo*.

El activismo pedófilo, aunque minoritario, no es nuevo y ha tenido un tradicional vínculo con Holanda, desde que el doctor en psicología Frits Bernard escribió su libro *Sexo con niños* (*Sex met kinderen*) en 1972 (cuando todavía CCC publicaba sus cortometrajes de la serie *Lolita*). En él recogía los estudios del Círculo del Enclave, que desde los años cincuenta proponía «eliminar prejuicios sobre temas relacionados con los contactos eróticos y las relaciones entre menores y adultos, y para proporcionar información y consejo así como iniciar un programa de asistencia directa». La famosa NAMBLA (Asociación Norteamericana para el Amor Hombre/Niño, por sus siglas en inglés) nació en esa misma década, en 1978, y en los ochenta obtuvo una cierta notoriedad para una organización tan pequeña, con algo más de trescientos miembros en aquella época, por las manifestaciones en su contra. La irreverente serie de animación *South Park* le dedicó un episodio en el que los retrata como peligrosos depredadores para niños ocultos tras un halo de legalidad aparente.

El apoyo a la pedofilia, que obtuvo un cierto reconocimiento entre las comunidades homosexuales, decreció hasta casi extinguirse en los ochenta y noventa hasta la llegada del Partido del Amor Fraterno, la Libertad y la Diversidad (PNVD por sus siglas en holandés) en el año 2006 en los Países Bajos. Los principales puntos programáticos eran despenalizar la tenencia y distribución de imágenes de

explotación sexual de menores —con el viejo y falso adagio de que quien lo consume no ha hecho daño a nadie—, tolerar la zoofilia y permitir el «amor entre hombres y niños». Utilizaban otro argumento falaz, que el infante tiene deseo sexual porque manipula sus genitales o sonríe si un adulto se lo hace. Esta racionalización de su deseo —«le busco una justificación lógica a lo que de todas formas voy a hacer» en vez de «analizo lo que pasa y llego a conclusiones por medio de ensayos»— es desmentida por cualquier pediatra o psicólogo infantil. Las fases de conocimiento del propio organismo no tienen que ver con una naturaleza erótica de la que el preadolescente carece. Otros puntos polémicos incluían la despenalización de las drogas blandas desde los doce años y las duras desde los dieciséis. Sus tres fundadores fueron Marthijn Uittenbogaard, Norbert de Jonge y Ad van den Berg. El último de ellos, que había pasado por la cárcel por abusar de niños en 1987, fue de nuevo detenido en 2010 y en su casa se encontraron grandes cantidades de pornografía infantil. Salió de prisión en 2014 y concedió varias entrevistas espeluznantes en las que afirma cosas como: «La mayoría de las veces no [he penetrado a los niños]. Hay estudios que dicen que la penetración es positiva solo en relaciones a largo plazo» o «creo que cuando se prohíbe el sexo, el alcohol y todas esas cosas, los niños se vuelven traviesos». Al final, el PNVD se disolvió en 2010, tras ser incapaz por dos veces consecutivas de obtener las seiscientas firmas preceptivas para poder presentarse a las elecciones en su país.

El activismo pedófilo a cara descubierta es menos preocupante que el más habitual en la red, aquel en que los miembros solo se identifican por un apodo y cuya idea es darse apoyo recíproco, nada más. Un individuo con tendencias pedófilas que se encuentre rodeado —aunque sea en la red— de otros que le explican que lo suyo «no es malo», que «en unos años será aceptado como hoy lo es la homosexualidad», le están quitando trabas morales para que decida lanzarse al abuso. Estas comunidades pedófilas son muy cuidadosas y no transgreden la legalidad ni permiten que terceros lo hagan en sus servidores. En la actualidad, una de las más activas es la que hemos mencionado más arriba, *boychat.org*, que mantiene el formato de un foro tradicional y en el que se pueden encontrar consejos sobre qué hacer si la policía registra la vivienda o resultados detallados de operaciones policiales, en especial quiénes han conseguido librarse de la condena y cuáles no y los motivos que han llevado a esas sentencias. Tras el desmantelamiento de Azov Films, del que hemos hablado antes y que se mantuvo más de un año en secreto, en Boychat fueron uniendo indicios hasta constatar que se estaba deteniendo a los compradores de aquellas películas y realizaron un exhaustivo estudio que puede leerse en su web.

OTROS DELITOS SEXUALES: DE CHANTAJES A ZOOFILIA

Con el Código Penal que entró en vigor en julio de 2015 pasó a estar penada por

primera vez la zoofilia, ya que el artículo 337 castiga la explotación sexual de un animal doméstico o amansado. Eso no incluye la distribución o tenencia de ese tipo de imágenes, como sí ocurre en otros países vecinos, como Alemania, Países Bajos o Reino Unido. Por ello, poseer o intercambiar ese tipo de material sigue siendo válido; no así la producción, puesto que se estará entrando en el tipo penal. Para grabar una relación con uno de nuestros primos de cuatro patas, esta tiene que producirse, que es lo que castiga nuestra legislación. Un informe presentado al Congreso por la Coordinadora de Profesionales para la Prevención de Abusos indica que hasta el sesenta por ciento de pederastas y el ochenta y uno por ciento de otros agresores sexuales han practicado zoofilia. Además, deja patente que en muchos casos de maltrato familiar, el agresor viola al animal doméstico como forma de «castigo» a su mujer o al niño.

La zoofilia es, por lo demás, un pujante negocio en Internet, con multitud de portales dedicados a la venta de ese tipo de material, además de la notable cantidad de pornografía gratuita que existe sobre el particular. Por supuesto, esto tiene su reflejo en los servicios anónimos de la red TOR, donde hay páginas, rizando el rizo, de necrozoofilia, esto es, donde se tortura y mata animales antes, durante o después de tener sexo con ellos, como NecroZoo o Animal's Nightmare (pesadilla animal en inglés).

Lo que puede preocupar hoy más a un adulto medio, sea hombre o mujer, es la conocida como *sextorsión*, acrónimo de «extorsión sexual». Grupos organizados, a menudo radicados en el norte de África y el Este de Europa, tienen contratados a hombres y mujeres que se dedican a buscar incautos solitarios por correo electrónico y por las redes sociales. Muchos ciudadanos han recibido un correo en que una hermosa dama o bello efebo afirman haberlo conocido en algún lugar no especificado y les proponen seguir hablando. Si el *primo* pica, establecerán una relación de *amistad* que pronto evolucionará hacia sesiones de cibersexo. Sin el conocimiento de la víctima, actuando igual que los *groomers* que ya hemos visto más arriba, grabarán el vídeo de lo que ocurre y, a partir de ahí, el chantaje pasa a mano de otros miembros de la organización, que van a pedir el pago de cantidades cada vez más altas para no revelar el material del que disponen. Hay que tener en cuenta que las víctimas pueden ser personas con familia, a menudo casadas, a las que su infidelidad virtual puede salirles muy cara.

Como de este delito todos podemos ser víctimas, debemos tener en cuenta que las posibilidades de haber ligado con una belleza espectacular de la que no recordamos nada son, como poco, escasas. Aun así, el sufrimiento que podemos tener nunca será, ni de lejos, parecido al de todos los niños víctimas de abusos sexuales que están siendo expuestos en Internet para el deleite de los más depravados.

3

LA GUERRA NO CONTEMPLADA

Maher[1] es iraní. Es alto, moreno y luce un rostro afeitado a la perfección, lejos del estereotipo habitual que de su gente tenemos en Occidente. Viste de manera impecable y sus zapatos están impolutos. Hubo un tiempo, en la época de Jomeini, en que un calzado sucio mostraba afección a la Revolución. Todo eso quedó atrás. Estamos en 2010 y él es un técnico nuclear, formado y correcto, que trabaja en el hipervigilado laboratorio subterráneo que el gobierno mantiene en Natanz, un área montañosa a más de trescientos kilómetros al sur de Teherán. En él enriquecen uranio para conseguir una energía atómica que saque a su país del siglo XX. Es un hombre orgulloso de los progresos de su nación y, al mismo tiempo, con la suficiente inteligencia para no creerse muchos de los bulos que emiten las agencias oficiales de noticias. Sabe que son necesarios para mantener enardecida a la población, por ello no los discute. Se limita, si está solo, como en su coche, a encogerse de hombros y sonreír. También es consciente de que la cantidad de isótopos que están obteniendo es muy superior a la necesaria para la utilización civil. Van a construir una serie de bombas para poder hablar de tú a tú con los judíos y las superpotencias.

Su mujer no está tranquila. Le pagan bien, pero el riesgo es muy alto. Hace poco que han asesinado al profesor Masoud Alimohammadi al hacer explotar una moto bomba al paso de su vehículo particular. Trabajaba en la universidad. Su aportación al programa nuclear era tan solo teórica. Aun así, esos malditos sionistas habían acabado con su vida. El asesino material, un tal Majid Jamali Fashi, feo, cejijunto, de veinticuatro años, había sido ya detenido y no tardaría en reconocer que recibía dinero del Mossad, el servicio secreto israelí. Morirían más científicos, pero él estaba dos escalones por debajo. Era uno de muchos jóvenes contratados y no era práctico asesinarlos a todos. Saludó al oficial de guardia que le franqueó el acceso al recinto mientras sus ojos se fijaban en los cañones antiaéreos que lo rodeaban. Las instalaciones estaban excavadas en la roca viva. Ningún arma diseñada por el hombre podría penetrar a tanta profundidad como para afectarles.

A las ocho en punto, como cada mañana, se sentó frente a la centrifugadora Siemens Simatic S7-300. Tras la consola, separados por un vidrio de seguridad, se extendían cientos de tubos en los que se inyectaba el gas más pesado conocido por el hombre, el hexafluoruro de uranio. Mediante la rotación de alta velocidad, los isótopos más pesados, los U238, quedaban en los extremos y eran desechados, mientras que los más ligeros, los radiactivos U235, flotaban en el centro del aparato y eran recolectados con mimo. Componían el material necesario para entrar en el selecto club de las armas atómicas.

Por un momento, pensó que algo iba mal. Parecía que la máquina hacía ruidos

raros. Sin embargo, los indicadores de velocidad eran todos los correctos, entre 807 y 1210 hercios, dentro de los parámetros que la empresa fabricante, la nacional Fararo Paya, consideraba óptimos. Después de diez minutos, tuvo la certeza de que había algún terrible error, por los ruidos y quejidos. El monitor no estaba dando los datos correctos. Un olor a cable quemado invadió el área mientras el característico silbido cada vez más grave indicaba que los motores eléctricos de cada centrifugadora se habían averiado. Maher pulsó el botón de emergencia. El personal comenzó la evacuación y todos salvaron la vida —o, al menos, se libraron de una contaminación radiactiva— por los pelos. Fuera lo que fuese lo ocurrido, había sido tan devastador y efectivo como un bombardeo. No sabía cómo, pero tenían que haber sido los sionistas.

No le faltaba razón. Las instalaciones habían sido víctima de uno de los pocos ataques de ciberguerra concebidos como tales, el virus Stuxnet, un prodigio de programación desarrollado por Israel y Estados Unidos tan solo para atacar ese tipo concreto de centrifugadoras.

El programa nuclear iraní acababa de ser detenido en su totalidad por meses.

LA GUERRA SIN REGLAS

En 1983, John Badham dirigió la película *Juegos de guerra*, con un joven Matthew Broderick en el papel de un *hacker* adolescente que consigue infiltrarse en la red de defensa nuclear de Estados Unidos y está a punto de desatar la tercera guerra mundial. La película resultó en cierta medida profética y eso en un mundo que todavía no concebía la interconexión actual, donde hasta los frigoríficos acceden a Internet.

Por supuesto, no es tan fácil acceder a una red de defensa militar o a otras infraestructuras críticas, porque ese tipo de instalaciones *no están conectadas a Internet*. En el mejor de los casos, disponen de dos redes diferentes que no comparten ningún vínculo; una, la que controla los sistemas críticos y otra, con Internet, para ordenadores de oficina. Esta es, por tanto, vulnerable, pero el daño que puede sufrir es más limitado. Pueden llegar a robar datos de los usuarios, aunque los piratas no pueden, por ejemplo, lanzar misiles intercontinentales. Como ya vimos en el primer capítulo, haría falta una conexión física, como ocurrió en los noventa en Estados Unidos —ir al hospital y pinchar sus cables— para conseguir ese acceso.

La definición de ciberguerra o guerra cibernética no está clara. No puede ser considerada bélica cualquier acción que un país realice sobre otro. Después de los sucesos de Estonia en 2007, de los que hablaremos más adelante, los expertos de la OTAN desarrollaron el Manual de Tallín sobre la legislación aplicable a esta materia. En él se definen una serie de puntos que se pueden resumir en dos:

1. Un ciberataque debe poder asimilarse a una «acción armada» y, por tanto, tener el objetivo de matar, herir o destruir físicamente propiedades. Por tanto, una denegación de servicio —que no funcione una página web durante un tiempo, por ejemplo, algo al alcance de cualquier grupito de chavales con conocimientos de informática— o el robo de datos —como planes de defensa o el nombre de agentes secretos— no se pueden considerar de esta categoría.
2. Un estado ha de ser responsable de atacar a otro. No es suficiente con que elementos incontrolados de una determinada nación intenten hacerlo, sino que deben estar respaldados por el gobierno de la primera de forma inequívoca (como militares de derecho o, al menos, asimilables, en el caso de *hackers* contratados por las Fuerzas Armadas).

La naturaleza del espacio digital es muy diferente a lo conocido hasta ahora y plantea muchas dudas y, más aún, dificultades para asociar hechos con autores. En este nuevo campo de operaciones no hay soldados capturados o muertos, no hay aparatos derribados y, a veces, las acciones cometidas un día pueden tener efectos muchas semanas o meses después sin el control de quien lo ha ejecutado, incluso después de que las batallas hayan acabado. Los límites de la ciberguerra son muy difusos. ¿Un grupo independiente que no es perseguido por su gobierno y que ataca a un país con el que tiene un conflicto se puede considerar en el tipo? ¿La propaganda en Internet y la desmoralización del «enemigo» lo son? ¿Y el perjuicio económico a una gran empresa, como Sony?

En un sentido amplio, podemos considerar ciberguerra todo acto entre dos países que tenga su origen en una disputa entre naciones y que esté respaldada por ellas. Esto lo diferencia del ciberterrorismo —que busca la desestabilización o hacerse visibles—, del crimen organizado —que busca beneficio económico o poder— y del *hacktivismo* —que se mueve por patrones ideológicos utópicos o por venganza.

La ciberguerra no está contemplada en la Convención de Ginebra. Por ello, sus acciones son ilimitadas: ataques a la población o a servicios humanitarios podrían ser llevados a cabo por los beligerantes. El Manual de Tallín pretende poner algunas reglas —como no atacar hospitales, por ejemplo—. Sin embargo, es un documento *de parte*, recomendado a los miembros de la OTAN. Los países más activos en estas lides, Rusia, China y Corea del Norte, no lo reconocen. Esto puede evolucionar en una suerte de *guerra fría digital* de consecuencias imprevisibles. Es el resultado de una tecnología que avanza diez veces más rápido que la legislación que debe regirla.

Los actos que se pueden llevar a cabo hoy en una ciberguerra son ya lo bastante dañinos. Dejando a un lado la propaganda, el caso más habitual y que menos formación necesita son ataques de denegación de servicio que desconecte de Internet páginas web —por ejemplo, las agencias de noticias—. En caso de conflagración, una desinformación brusca achacable al enemigo puede tener un importante efecto en los civiles y en la moral de las tropas. Con las herramientas adecuadas se puede ir un

paso más allá y desconectar emisoras de televisión o de radio. Suelen ser uno de los objetivos habituales en las campañas aéreas, como el ataque a la Radiotelevisión Serbia llevado a cabo por Estados Unidos y sus aliados el 22 de abril de 1999, que dejó dieciséis muertos. Hubiera sido menos sangriento poder hacerlo a distancia. Incluso, de una manera egoísta, no hubiera representado riesgo para los aviones propios que tuvieron que internarse en territorio hostil. Una vez que se ha conseguido el control de una estación se puede usar a favor del atacante, difundiendo noticias falsas o engañosas.

Las comunicaciones militares están encriptadas y utilizan protocolos de alta seguridad. El estándar actual de la OTAN, llamado Link 16, proporciona datos en tiempo real a toda la red de defensa y ataque. No solo voz o texto, sino también imágenes, vectores, posiciones y, en general, toda la información del campo de batalla. Los aviones en ruta van recibiendo actualizaciones sobre sus objetivos; los barcos, la señal de los helicópteros sobre los submarinos enemigos, etc. La OTAN utiliza para ello la banda de radio 960 a 1215 MHz (banda L) y, además, puede usar TCP/IP —como Internet—. Está pensada y diseñada para resistir ataques. Si un enemigo pudiera interferirla o, mejor aún, inundarla de datos falsos, paralizaría de forma inmediata toda la actividad aliada so pena de ser destruidos. Ningún soldado puede hacer la guerra moderna de forma aislada. Por ejemplo, en los combates del valle de Bekaa (Líbano) entre Israel y Siria en 1982 (Operación Mole Cricket 19), los israelíes consiguieron bloquear por completo las transmisiones árabes mientras ellos mantenían todas sus capacidades. Como resultado, destruyeron ochenta y dos aviones y treinta baterías de misiles antiaéreos sin sufrir bajas de relevancia.

Ciberataques más complicados —porque sus sistemas, como decíamos al principio, no deberían estar conectados a Internet— se pueden llevar a cabo contra centrales productoras de energía o de distribución de la misma, con lo que es posible dejar a oscuras grandes áreas. Si se accede a las compuertas de una presa se pueden inundar ciudades enteras y si se alcanzan los controles de una estación nuclear, causar nuevos *fukushimas* a voluntad. Estos tipos de ataque no son baratos. En Estados Unidos hicieron un ejercicio militar de ciberguerra llamado Digital Pearl Harbour en 2002, que llegó a la conclusión de que un ataque de esa clase era posible y factible, aunque requería una inversión de al menos doscientos millones de dólares. Esa cantidad es una minucia comparada con los presupuestos de los grandes países, incluso del nuestro. Unos años antes, en 1997, otro ejercicio cibermilitar, llamado Eligible Receiver demostró que las vulnerabilidades existen. Entre el 9 y 13 de junio, un equipo formado por los treinta y cinco mejores especialistas de la Agencia Nacional de Seguridad norteamericana asumió el rol de atacante y trató de hacer todo el daño posible —simulado— a diferentes instalaciones militares y civiles. Solo podían utilizar Internet y herramientas existentes, no desarrollar armas virtuales propias. Con esas limitaciones consiguieron lanzar exitosos ataques de denegación de servicio, manipular correos electrónicos para hacerlos pasar por legítimos y así

engañar a sus receptores, bloquear las comunicaciones militares e incluso, debido a la mala configuración de la seguridad, acceder a treinta y seis redes internas de organismos oficiales y borrar sus discos duros.

En resumen, las acciones de ciberguerra pueden ser de tres tipos:

A. *Robo de información*: debe llevarse a cabo para los propósitos de la guerra, no como espionaje industrial o mero *hacktivismo*. Consiste en obtener datos significativos del enemigo, desde planes de batalla hasta los nombres de agentes enemigos infiltrados o códigos para acceder a las comunicaciones encriptadas.

B. *Alteración de las infraestructuras, tanto civiles como militares*: el acto más simple es la denegación de servicio que ya hemos mencionado con anterioridad y de la que hablaremos con detenimiento en el capítulo ocho, esto es, conseguir desconectar una página web de Internet, de forma que nadie la pueda consultar. Un paso más sofisticado es sustituir el contenido presente por otro que interese al atacante, como noticias engañosas o falsas. También entra en esta categoría la desconexión del sistema de control de tráfico de una ciudad o el bloqueo de la bolsa de valores.

C. *Destrucción física de la propiedad*: según la definición restringida de ciberguerra, estos serían los únicos hechos que merecerían tal consideración. Esta destrucción puede ser directa —borrar o dañar unos discos duros o causar una sobrepresión de gas que lleve a una explosión— o indirecta —abrir las compuertas de una presa y causar una inundación.

DE TUBERÍAS QUE EXPLOTAN A CENTRALES NUCLEARES ARRUINADAS

No hay que entender este concepto como algo por completo separado de las demás ramas de lo militar. Todo está interconectado desde lo más básico. En el pasado, la ciberguerra estaba más cercana a la inteligencia que al campo de batalla. La Guerra Fría daba sus últimos coletazos cuando se llevó a cabo uno de los primeros ataques de los que se tiene noticia. Ocurrió en 1982, antes de que el común de los mortales entendiese la posibilidad de una red interconectada. Antes incluso de la película *Juegos de guerra*, que abrió los ojos a muchos y, por supuesto, antes de que la idea de Internet profunda tuviese sentido. Los entonces soviéticos robaron de una empresa canadiense un avanzado sistema de gestión automatizada para su gasoducto transiberiano. La complejidad del proyecto era excesiva para su tecnología, así que la KGB consiguió hacerse con el sistema informático que podía solucionarles la papeleta. El problema es que la CIA lo sabía y había implementado una *bomba lógica* —un programa que permanece oculto hasta que algo, una fecha, una instalación

determinada, etc., lo activa y entonces causa los daños que tenga en su secuencia—. Aquel, en concreto, al ponerse en funcionamiento modificaba la presión de las tuberías hasta niveles que superaban con holgura la tolerancia de la construcción. Causó la que, según algunas fuentes, ha sido la explosión no nuclear más grande de la historia, con una potencia de tres kilotones. Debido a que ocurrió en un área remota de Siberia, no causó víctimas.

Más tarde, en 1991, las víctimas cambiaron de bando. Transcurría la primera Guerra del Golfo cuando un grupo de adolescentes holandeses consiguió *hackear* el Departamento de Defensa de Estados Unidos y robar planes operacionales de la coalición —que no deberían haber estado ahí—, y luego intentaron vendérselos a los iraquíes, que los rechazaron porque pensaron que era un engaño. Este asalto, en puridad, no fue un acto de ciberguerra, puesto que quienes lo ejecutaron no eran parte de ninguno de los dos países.

En 1999, en la guerra de Kosovo, una entidad organizada, coordinada a través de Internet, realizó labores de ciberguerra, aunque a pequeña escala. Bajo el mando del controvertido *capitán* Dragan, héroe del conflicto contra Croacia, cuatrocientas cincuenta personas —ingenieros informáticos, periodistas, *webmasters*— con cuarenta ordenadores mantuvieron una activa labor de propaganda para desmentir las *mentiras* que Occidente vertía contra el pueblo serbio. Para ello contaban con varias páginas web y una estrategia más profunda, puesto que varios *hackers* independientes, sobre todo de Alemania y Rusia, se ofrecieron desinteresadamente para ayudarles de forma más directa. Aceptaron su ofrecimiento el 24 de marzo y al día siguiente ya se habían conseguido infiltrar en el sistema principal de la OTAN y el del portaaviones nuclear *Nimitz*. Se limitaron a sustituir fondos de pantalla por fotografías obscenas del entonces presidente Bill Clinton. Según Dragan, no fue algo muy efectivo, poco más que una demostración de fuerza y una advertencia —que poco efecto tuvo— en caso de que la campaña aérea que estaba teniendo lugar se convirtiera en una *guerra total*. Este *affaire* puso de relieve lo que iba a ser una de las constantes de la forma de actuar del Este de Europa, en especial Rusia. En vez de tener organizaciones dedicadas a la defensa informática —que también—, confían en adeptos a la causa, tanto de su país como de otros, a los que pueden llegar a pagar por sus esfuerzos.

Un paso más allá llegaron los ataques organizados que sufrió Taiwán en 2003. La pequeña isla del estrecho de Formosa está habitada por los perdedores de la guerra civil que llevó al poder a Mao Tse Tung en los años cuarenta. Para China, es parte integrante de su territorio, por lo que lanza amenazas regulares de incorporarla al mismo por la fuerza. En ese continuo estado de tensión, el país empezó a sufrir una serie escalonada de ataques que dejaron sin servicio la bolsa, los semáforos, la red viaria y, peor aún, hospitales. Aunque las autoridades atacadas señalaron a China —en concreto, a la Unidad 61398 del Ejército Popular, la dedicada a esos menesteres— como la única con la capacidad y la motivación suficientes para hacerlo, nunca se

logró demostrar y el gigante asiático negó toda responsabilidad. La lógica dicta que fue un ensayo de lo que se puede llevar a cabo para estragar la organización civil enemiga en caso de combate abierto. Se puso de manifiesto que el caos ralentizaría o detendría, al menos un tiempo, el esfuerzo bélico. No fue la primera vez ni será la última que en Taiwán sufren hechos similares, puesto que la antigua Formosa es el objetivo favorito para los experimentos de su poderoso vecino. A diario tienen que lidiar con cientos de ataques de mayor o menor entidad, sin que puedan averiguar cuáles son militares y cuáles provienen de *hackers* independientes o de redes criminales.

Algo parecido ocurrió en Estonia en 2007, solo que en este caso la ofensiva provino de Rusia y *tan solo* sufrieron denegaciones de servicio, aunque fueron tan masivas que la red nacional entera colapsó durante varias horas en uno de los países con un cableado más denso y sofisticado, capaz de soportar un tráfico mucho mayor que, por ejemplo, España o hasta Estados Unidos. El detonante fue el traslado de la estatua de un soldado soviético de la Segunda Guerra Mundial, que indignó a un grupo de atacantes, pertenecientes a la organización política pro-Kremlin NASHI, liderados por un chaval de veintidós años llamado Konstantin Goloskolov. Afirmaron que actuaron por su cuenta y el primer ministro estonio declaró que no se podía demostrar que las autoridades rusas estuvieran implicadas. Sin embargo, más tarde, uno de los integrantes del grupo aseguró haber recibido dinero del FSB, el sustituto del KGB.

Al año siguiente, durante la invasión rusa de Georgia, ocurrieron hechos similares, sobre todo contra prensa de aquel país. Aparte de algunos ataques típicos contra diversas webs —como poner fotografías de Hitler en vez de las del presidente georgiano—, la verdadera novedad la constituyó la sustitución de las páginas de noticias del país invadido por otras alojadas en Rusia. Para ello atacaron los servidores DNS —recordemos el primer capítulo de este libro—; de esta manera, a la hora de escribir *www.osinform.ru*, que fue uno de los sitios atacados, en vez de mostrarnos la página legítima, asociada a una IP determinada, nos mostraba la que está en otra IP, ubicada en Rusia o Turquía y que alojaba contenidos propicios al invasor. El ataque comenzó antes de la declaración de guerra y, tras el cese de hostilidades, casi un mes después, muchas de las páginas seguían desconectadas o mostrando información incorrecta. *Hackers* georgianos contraatacaron e intentaron tomar el control de Russia Today y de la agencia estatal RIA Novosti, aunque con poco éxito. Los rusos, por su parte, lanzaron también sus ciberarmas contra los periódicos de otros países que veían demasiado pro-georgianos, como los de Azerbaiyán o incluso medios rusos que no mostraban el suficiente compromiso patriótico. De nuevo, ambos gobiernos negaron cualquier tipo de responsabilidad y lo atribuyeron a particulares, aunque ya sabemos que por lo menos los rusos suelen estar financiados, además de tener una alta motivación política.

Actos como los que hemos repasado son continuos entre todos los países, aunque

en general de menor intensidad que los que hemos nombrado hasta ahora. A menudo es difícil distinguir si el propósito es de ciberguerra (fría) o si está relacionado con otras ramas del delito. Con la salvedad de la explosión del gasoducto transiberiano, hasta el momento todos los hechos que hemos referido son inmateriales. No han causado un daño físico mensurable y, cuando cesaron, los sistemas atacados volvieron a la normalidad. Casi todos, pues, pertenecen a la modalidad «B» de los arriba descritos. Ataques tipo «C» también ha habido, si bien pocos, porque causar la destrucción física de una propiedad es difícil y a menudo caro. Si este elemento es una infraestructura crítica no estará conectado a Internet y la infiltración habrá que hacerla de otra manera. Los cibersoldados tienen que estrujarse las meninges para lograrlo.

Israel es un país con una situación única en el mundo. Está rodeado de enemigos por todas partes y carece de territorio suficiente para poder realizar, en caso de ser atacado, una defensa en profundidad. Por ello deben estar siempre un paso por delante de sus vecinos. Sabe que el día que pierda una guerra, desaparecerá del mapa. Una de sus mayores preocupaciones es seguir siendo la única potencia nuclear en la zona. Por ello, en 1981 atacaron, en una incursión audaz, el reactor iraquí de tecnología francesa en Al Tuwaitha —que ya había sido bombardeado, con menos éxito, por Irán—. Con su destrucción paralizaron para siempre el programa de Saddam Hussein.

La siguiente amenaza estuvo en Siria bien entrado el siglo XXI. Los servicios de inteligencia hebreos sabían con seguridad que en la prefectura de Deir Ez-Zor, fronteriza con Iraq, se estaba construyendo un reactor nuclear de tecnología norcoreana con capacidad de producir bombas atómicas. Por ello, el 6 de septiembre de 2007 Israel llevó a cabo un ataque para destruirlas. Sus cazas F-15I y F-16I, apoyados por aviones de guerra electrónica —reactores ejecutivos G500 Gulfstream modificados— se adentraron en el Mediterráneo a baja cota antes de girar, cerca de la frontera siria con Turquía, hacia el interior. Una vez allí, atacaron con bombas de precisión un solo radar de defensa aérea y, de pronto, todo el sistema antiaéreo del país dejó de funcionar y se mantuvo así hasta que, tras destruir sus objetivos, los judíos volvieron a sus aeródromos. Los sirios habían adquirido en Rusia poco antes uno de los medios integrados contra aviación más sofisticados del mundo y se sentían protegidos ante las promesas de total invulnerabilidad. Según la publicidad, ningún avión podría pasar desapercibido ni escapar a los misiles superficie-aire de ultimísima generación. Claro que eso suponía que los radares estarían conectados. Este medio no violento de dejarlos fuera de combate intrigó tanto a los rusos que mandaron de inmediato a un grupo de especialistas para estudiar lo que había ocurrido. Aquí vemos un ejemplo de tipo «C», aunque sea indirecto. El ciberataque dejó desconectada toda posibilidad de defender las instalaciones de las bombas.

Los gobiernos sirio e israelí se pusieron de acuerdo —por extraño que parezca— para silenciar el incidente, utilizando como mediador al presidente turco, por lo que el

conocimiento de los hechos procede de terceras fuentes, en especial de Estados Unidos. Las conclusiones de los expertos del Kremlin, por supuesto, tampoco son conocidas. Algunas especulaciones sugieren que el Mossad reemplazó algunos microprocesadores de ordenadores auxiliares con ingeniería civil por otros que contenían una *puerta trasera*, una manera de permitir el acceso a un agente externo que conozca cómo hacerlo —una palabra clave determinada o un conjunto de acciones único, por ejemplo—. Esto es posible porque, para abaratar costes, es habitual complementar las instalaciones militares con equipos que se pueden adquirir en el mercado civil. Por su naturaleza, estos son más baratos, pero también es más fácil que hayan sido modificados por una potencia interesada. No obstante, lo más probable es que utilizaran una herramienta desarrollada por la constructora de aviones británica British Aerospace y conocida como Suter. La mayor parte de las características, hasta sus capacidades, son secretas, porque una vez que se conozcan será muy fácil desarrollar contramedidas. Lo que sí se sabe es que permite *hackear* desde el aire redes enemigas, en especial las antiaéreas. Para ello requiere, en primer lugar, una amplia base de datos sobre dónde están los emisores —los sensores enemigos— conocidos y cómo son esas emisiones, puesto que el espectro electromagnético es muy amplio y cada sistema funciona en una longitud de onda y con unos patrones únicos. Después, una muy potente capacidad de detección de las mismas, tanto activa —emitiendo ondas, como un radar— como pasiva —recibiendo las ondas que otros emiten—. En resumen, no puede hacerse «desde casa»; es necesario estar sobre el terreno en una aeronave preparada al efecto, con una dotación muy especializada, perteneciente a la Unidad 8200 de las Fuerzas de Defensa de Israel. De ahí la presencia de los Gulfstream junto a los cazas. Una vez lograda la intrusión, puede realizar tres acciones, cada cual más invasiva: monitorizar lo que los enemigos ven, tomar el control de la red atacada y desviar sus antenas o, como en el caso sirio, desconectar por completo la malla del objetivo. Suter era utilizado en Afganistán por una unidad secreta de la Fuerza Aérea de los Estados Unidos llamada Big-Safari, al menos desde 2006, porque es capaz de interferir dispositivos mucho más sencillos, como las señales de radio utilizadas por los talibanes para activar sus explosivos improvisados al paso de los convoyes aliados. Si fue esto lo que usaron los israelíes, una modificación o un diseño propio quizá nunca se sepa.

El uso de Suter había puesto muy nervioso a otro país de la zona, Irán. Desde el año 2002 estaba llevando a cabo su propio programa nuclear, más complejo y más avanzado que el sirio y protegido también por el mismo sistema de mando y control que había sido desactivado con tanta facilidad. Los expertos rusos no supieron darles una respuesta precisa sobre lo que había pasado, lo que les desagradó sobremanera. El país de los ayatolás no era el de su aliado Al-Assad, sino mucho más grande y con más recursos. Sus instalaciones estaban excavadas en la roca viva de las montañas de Natanz, tan profundas que ningún ataque aéreo las podría dañar. No hay mejor defensa contra las armas de los hombres que la propia naturaleza y nada amortigua

tanto una explosión como la roca y la tierra. Además, las repercusiones diplomáticas no serían las mismas, sobre todo desde que el presidente Obama de los Estados Unidos había optado por las sanciones económicas y el embargo, al que se habían unido casi todos los países occidentales.

Israel, por supuesto, no pensaba detenerse y realizó una campaña de asesinatos de destacados ingenieros nucleares persas, como el profesor universitario Masoud Alimohammadi, un hombre versado en su materia pero que nada tenía que ver con el enriquecimiento de uranio. A ese nombre seguirían otros: Dariush Rezainejad, Mostafa Ahmadi Roshan o el de Fereydun Abbasi, que escapó herido a una bomba. El primero de todos fue, en 2007, Ardeshir Hoseinpur, especialista en electromagnetismo y trabajador en una de las plantas de conversión de uranio.

Mientras los servicios secretos civiles llevaban a cabo su campaña de asesinatos selectivos, la Unidad 8200 estaba trabajando por otro camino. Esta es la organización militar judía más grande, con varios miles de soldados trabajando en ella. Su función es la monitorización, captación y análisis de información electrónica para propósitos de contrainteligencia. En esencia, su función es *oír* todas las emisiones de los países vecinos —transmisiones militares, ondas de radar o de radio, etc.— para saber cómo usarlas en su provecho. En ocasiones esa escucha puede prevenir un ataque o un atentado y en otras conseguir datos sobre cómo se despliegan las fuerzas contrarias o cuáles son los huecos que no tienen cobertura.

Los Estados Unidos querían evitar a toda costa un ataque aéreo que pudiera desequilibrar una región que llevaba siglos siendo bastante problemática, más aún desde su intervención en Iraq a partir de 2003 que todavía mantenía a finales de la década a miles de sus soldados como fuerza de ocupación. Por ello ofrecieron a Israel la opción de desarrollar un *gusano* que destruyese las instalaciones iraníes desde dentro y con la misma efectividad que si explotase una bomba en ellas. Así nació la Operación Juegos Olímpicos, en la que solo por parte de Estados Unidos se invirtieron trescientos millones de dólares y tres años de trabajo antes de lograr algo utilizable. Un equipo multidisciplinar de ambos países se dedicó a crear la herramienta más sofisticada y especializada que ha tenido nunca la naciente guerra informática, *Stuxnet*. No querían fallar, así que se emplearon a fondo. Estaba diseñada en varios lenguajes de programación diferente y su código era más complejo y perfecto que el habitual en los virus creados por delincuentes. Utilizaba cuatro vulnerabilidades —hasta veinte según algunos expertos— conocidas como *día cero* —aquellas que empiezan a ser explotadas sin que el programador tenga conocimiento de ellas, por lo que ha tenido *cero días* para preparar un parche o actualización—. Dado lo valiosos que son esos errores, no suele emplearse más de uno por programa, porque, una vez conocida la existencia del *bug*, como se conoce en argot informático, se desarrollarán con velocidad parches que evitarán que puedan seguir siendo usadas. Encontrar y malgastar cuatro a la vez no es algo que le salga rentable a una organización criminal. Los gobiernos son harina de otro costal.

Debía diseminarse fuera de Internet para tener alguna oportunidad de llegar a su destino, así que decidieron que su propagación se llevaría a cabo a través de memorias USB como las que hoy en día casi todos llevamos en el bolsillo. *Stuxnet* se instalaba en cada ordenador de tal manera que no era detectado por el sistema operativo y luego se replicaba de dos maneras. Por un lado, si el ordenador estaba en una red interna, como la que tienen la mayoría de las empresas, se copiaba en todos los elementos que la compusieran. Por el otro, cada vez que alguien pinchase un *pendrive*, se llevarían una copia inadvertida. Bastaba, pues, introducir el programa en ordenadores iraníes para que antes o después llegase a las instalaciones nucleares.

El gusano, aparte de copiarse, no hacía nada más, salvo que se dieran tres circunstancias, que se utilizara un sistema operativo Windows, que tuviera instalados unos programas determinados de la empresa Siemens y que al mismo estuvieran conectadas centrifugadoras nucleares S7-300 de esa misma empresa, que eran las que había comprado en el mercado negro —era un producto sujeto a embargo internacional— Irán. Solo en ese caso se activaba. Se dedicaba a cambiar de manera brusca la frecuencia de centrifugado, de muy despacio a muy rápido y vuelta a empezar y, a la vez, seguía enviando señales de que todo estaba funcionando según los parámetros habituales. De esta manera consiguieron destruir más de mil centrifugadoras, el diez por ciento de las existentes, y detener durante unos meses el programa nuclear hasta que pudieran averiguar qué estaba pasando. La Operación Juegos Olímpicos había tenido éxito… y continúa, ya que dos años después, una central térmica del sur del país resultó afectada por una variante del virus.

Los analistas iraníes lo encontraron y fueron capaces de neutralizarlo mediante programas dedicados. También Siemens proporciona un archivo de desinfección a todos los clientes que lo necesiten. El gigante de la seguridad informática Symantec calcula que el sesenta por ciento de todos los ordenadores afectados en el mundo está en Irán. La compañía de antivirus VirusBlokAda, basada en Bielorrusia, fue la primera en detectarlo fuera de las fronteras iraníes, en 2010. No obstante, los objetivos de *Stuxnet* están conseguidos. Todo lo que ocurra desde ahora es tan solo un bonus.

No podemos acabar una historia dedicada a la ciberguerra sin hablar del país más hermético y que más ríos de tinta especulativos hace correr: Corea del Norte. Bajo la férrea tiranía de la dinastía comunista Kim, la población no tiene acceso a las comodidades más básicas en el mundo occidental o en Asia —por ejemplo en su vecina del sur— como, por supuesto, Internet. Un país de veinticinco millones de habitantes apenas cuenta con mil doscientas direcciones IP asignadas —y, recordemos el capítulo uno, ya no quedan más disponibles—. Aun así, parece que el total de direcciones utilizadas de forma oficial es todavía más limitado. La Universidad de Ciencia y Tecnología de Pyongyang solo tiene una IP y apenas hay unas treinta webs oficiales, todas ellas operadas por el gobierno. De hecho, hasta 2009, la única manera de acceder a Internet en la República Popular era a través de

una conexión satélite con Alemania, reservada, como es obvio, para las más altas funciones gubernamentales. En 2010 inició sus servicios una empresa llamada Star Joint Venture, participada por la Compañía Nacional de Telégrafos y la mercantil tailandesa Loxley Pacific. La inmensa mayoría de los norcoreanos solo puede acceder a una Intranet privada que abarca todo el país, de uso gratuito —a través de centros oficiales, puesto que tener un ordenador en casa está más allá de lo imaginable para la mayoría—. Se llama Kwangmyong (Brillante, en español), contiene información y datos enciclopédicos controlados con firmeza por los censores, y no está conectada al Internet global.

Con estos antecedentes, resulta extraño saber que en enero de 2015, la Oficina 121, el organismo que tiene atribuida la responsabilidad de la ciberguerra, tenía seis mil militares trabajando en ella. Según algunos medios surcoreanos, la Universidad Kim Il-Sung está formando a más expertos en seguridad informática. Debemos entender que en Corea todo está supeditado a las necesidades del gobierno, en especial a las militares, dado que la guerra de los años cincuenta contra Corea del Sur y sus aliados de las Naciones Unidas nunca ha acabado de forma oficial. Basta consultar cualquier mapa de ciberataques en tiempo real para observar que una fracción importante de la actividad agresiva de todo el mundo tiene origen o destino en el norte de Corea.

Uno de los objetivos de la Oficina 121, como no podía ser de otra manera, son sus vecinos de península. Destaca el ataque llevado a cabo en 2013 contra estaciones de televisión y bancos de aquel país, que causó interrupciones en el funcionamiento de muchos ordenadores, incluidos cajeros automáticos y banca electrónica. Otros similares, aunque con menos repercusión, ya habían ocurrido en los dos años impares anteriores. El conjunto de técnicas y herramientas que se utilizaban para ello recibió el nombre de *DarkSeoul* (Seúl oscuro).

La opinión pública conoció de golpe la actividad en la red de las tropas de Kim a finales de 2014, con el *affaire* de Sony Pictures, una de las productoras de cine más importantes del mundo. Por aquel entonces estaban a punto de estrenar una película llamada *The Interview* (*La entrevista*), una comedia sobre dos periodistas estadounidenses que acudían a entrevistar al líder norcoreano y se veían envueltos en una conspiración para su asesinato. La sinopsis gustó tan poco a aquellas autoridades que llegaron a protestar de forma oficial ante la ONU, con poco éxito. Incluso el director ejecutivo de la multinacional japonesa, Kazuo Irai, presionó, sin lograr nada, para que se rebajase la violencia de la muerte del dictador, temeroso de las posibles reacciones.

El día 24 de noviembre de aquel año, un grupo de *hackers* que se hacían llamar a sí mismos Los Guardianes de la Paz avisaron de que habían obtenido hasta cien *terabytes* de información de Sony. Además, habían implantado en sus sistemas una ciberarma llamada *Wiper* (Barredor), destinada a borrar todos los discos duros que habían infectado, destruyendo así documentación de un valor incalculable, como los

originales de películas aún por estrenar. En días sucesivos fueron filtrando elementos obtenidos, como correos electrónicos privados intercambiados por gerifaltes de la compañía y que desvelaban negociaciones con actores o comportamientos no muy edificantes, cuando no directamente racistas. A cambio de dejar de revelar información, el grupo pedía que no se estrenase la película en cuestión y, más adelante, lo mismo que había indicado Kazuo Irai unos meses atrás, que se suavizase el asesinato fingido de Kim. Al poco, filtraron el final de la película, para desesperación de los directivos de Sony. Estos, por fin, decidieron acceder y *The Interview* nunca se distribuyó de forma masiva. En lugar de eso, se estrenó en la Navidad de aquel año en trescientos cines independientes de los Estados Unidos y, en febrero de 2015, salió a la venta en Blu-Ray. De los cuarenta y dos millones de dólares que costó, apenas recuperó doce. Además, la multinacional ha gastado al menos otros quince en recuperarse del daño causado a sus sistemas. Así pues, estamos ante un ataque del tipo «A» con algunos toques de «C». Lo que queda es definir si estamos ante un acto de ciberguerra o un mero ataque criminal.

Estados Unidos no tardó en acusar a Corea del Norte por estos hechos, incluso el presidente Obama declaró que lo incluía entre los países patrocinadores del terrorismo. La nación asiática no tardó en responder, fiel a su retórica habitual, con una cuasi-declaración de guerra. Negaron toda involucración en los hechos y, al mismo tiempo, ofrecieron toda la ayuda que necesitasen investigadores independientes para esclarecer la verdad. Una actitud similar a la rusa en los casos que ya hemos visto, salvo que en el país de Kim no hay libertad alguna para que existan grupos con Internet en sus domicilios que puedan organizarse y atacar. Lo hace el Estado o no se hace.

El FBI concluyó que el ataque provenía de Corea del Norte porque el método con que se había realizado era muy similar al de otros que se sabía que provenían de allí, igual que las redes utilizadas —solían usar para ello empresas del sur de China—, las líneas de código y los algoritmos, que eran casi calcados a los de *DarkSeoul*.

Sin embargo, algunos expertos independientes afirmaron que la única explicación lógica era que fuera un «trabajo desde dentro», llevado a cabo por antiguos empleados que se sentían perjudicados por su salida de la compañía. Esto parecía reforzado por la estimación de que, para obtener los cien *terabytes* de datos de los que afirmaban disponer, habría hecho falta al menos que el ataque hubiera durado un año entero sin ser detectado, mucho antes de que la producción de la película en cuestión fuera de conocimiento público. El FBI desestimó esas afirmaciones. Sus conclusiones seguían siendo las mismas.

Como vemos, todas las naciones con capacidad están llevando a cabo acciones que se pueden considerar ciberguerra cada vez que lo consideran necesario. Además, amparándose en la dificultad de identificar a los autores, los gobiernos a menudo niegan su responsabilidad, hasta que las evidencias, las raras veces que las hay, son irrefutables.

Los países que están en condiciones de ello mantienen grupos gubernamentales de defensa informática, como la Unidad 61398 china o la Oficina 121 norcoreana. La agencia alemana de Inteligencia, el BND, tiene al menos 130 *hackers* contratados y en Estados Unidos la protección informática forma parte de los *cinco pilares* de su estrategia defensiva. Irán e India son dos potencias emergentes en este ámbito, en el que Rusia es todo un veterano.

Además, para ciertas operaciones se recurre a terceros, de manera que se pueda negar, de forma más o menos plausible, responsabilidad nacional. Ya hemos visto que el país de Putin es uno de los que más recurren a ello, incluso a través de la subvención directa por parte de sus servicios de espionaje, siempre a personal que en primer lugar tiene una alta motivación ideológica.

En España, la defensa general contra todo tipo de ciberataques recae en el INCIBE, el Instituto Nacional de Ciberseguridad, con sede en León. Es un organismo participado por la Administración y la empresa pública *Red.es* y en él trabajan, entre otras personas, setenta informáticos con una alta especialización en seguridad. Son ingenieros de telecomunicaciones, matemáticos y físicos, todos ellos con un amplio bagaje y formación. Son pocos, muy pocos, y esperan que su número aumente en próximos años, dado que las necesidades y los ataques crecen a un ritmo vertiginoso. En los seis primeros meses de 2015 hubo veintitrés mil ataques contra nuestro país. En 2014, último año del que se tienen datos a la hora de escribir estas líneas, hubo dieciocho mil contra individuos o entidades de nuestro país. De estos, quinientos tuvieron por objetivo infraestructuras críticas, como la banca, suministro de agua, puertos y aeropuertos o redes telefónicas. Destacan cuatro contra centrales nucleares y otros tantos contra industrias energéticas, ninguno de ellos de alto riesgo, así como el intento de controlar los teléfonos de cuatro altos miembros del gobierno. La mayoría de los ataques provienen de Rusia y China. El ministro de Asuntos Exteriores, García Margallo, denunció que España es el tercer país que más ciberataques sufre en todo el mundo, después de Estados Unidos y Reino Unido. La inmensa mayoría de las veces no se corresponden con casos de ciberguerra, sino con delincuencia *normal*, como el robo de credenciales bancarias o de datos almacenados en un equipo. Son más peligrosos los intentos de tomar el control de un ordenador *sensible* y así introducirse en un sistema informático. Los ataques de denegación de servicio, aunque comunes, son más una molestia que un riesgo cierto.

Los profesionales españoles deben pasar duras pruebas de acceso para trabajar en INCIBE, como saber *colarse* en una red protegida, detectar vulnerabilidades, descubrir cómo se ha construido un *malware* a partir de sus efectos —la denominada ingeniería inversa— o saber realizar análisis forense de incidentes.

YIHADISMO E INTERNET: CUANDO LA DOCTRINA CHOCA CON LA NECESIDAD

El endurecimiento del Código Penal de España en 2015 convierte en delito el hecho de consultar webs de contenido yihadista de forma habitual, por lo que, como en el capítulo anterior, recomiendo a los lectores que se abstengan de buscar esos contenidos para evitarse posibles disgustos.

Con el advenimiento del nuevo milenio, el fundamentalismo islámico ha experimentado un notable auge. Las interpretaciones más estrictas del Corán han ganado preeminencia en muchos países de la franja que va de Egipto a Paquistán y Afganistán.

El Islam es más que una religión, está destinado a regir toda la vida del creyente, la interior y la exterior, la política y la espiritual. Esta aproximación holística hace que sea muy difícil una democratización al estilo occidental. El judaísmo y el cristianismo han implantado la separación Estado-Iglesia. Entre los musulmanes no existe tal distinción, porque es herética.

No es tampoco una religión unida. Si bien todos sus fieles profesan las mismas creencias básicas, hay dos ramas principales, la mayoritaria suní, que representa el ochenta por ciento de los creyentes, y la chií, que apenas supera un diez, centrados casi en exclusiva en Irán, zonas de Iraq y Siria. Desde que se estableció el cisma, en el año 680, con la batalla de Kerbala —ganada por los primeros—, ambos grupos no han parado de matarse a la menor ocasión. Aunque hay diferencias menores, la principal consiste en la autoridad que los minoritarios dan a sus imanes, que consideran guías infalibles de la comunidad y, por tanto, tienen un mayor poder de influencia sobre el pueblo. Un chií irá o dejará de ir a la guerra santa si sus líderes religiosos se lo ordenan. Las organizaciones terroristas con estas raíces, como la libanesa Hezbolá, mantienen una jerarquía que la hace actuar al unísono, sin sorpresas.

El sunismo, por contra, no reconoce intermediario entre Dios y los hombres. Cada cual debe interpretar el camino a la salvación siguiendo los seis pilares del Islam, uno de los cuales es la *yihad* o guerra santa. Dentro de esta corriente es aún más duro el wahabismo, mayoritario en Arabia Saudí, que supone un cumplimiento estricto de la *sharia*, ley islámica que no se diferencia mucho de códigos de justicia medievales europeos y que implica mutilaciones y decapitaciones por *crímenes* como la homosexualidad o el adulterio. Su otra característica es el expansionismo radical de su fe por todo el mundo, por la fuerza si es necesario.

Los dos grupos terroristas más peligrosos del siglo XXI pertenecen, por tanto, a esta facción. El primero, el celebérrimo Al Qaeda, fue fundado por el multimillonario Osama Bin Laden, ya fallecido, para oponerse a la invasión soviética de Afganistán en los años setenta y ochenta y, desde ahí, evolucionó a sus posiciones antioccidentales de hoy. No hay que entenderlo como una organización cerrada con mando sobre todos sus acólitos. Ya su propio nombre, que se podría traducir como «La Base», en su acepción de grupo de creencias básicas a seguir por los militantes, nos indica su propósito. Para ser miembro de la red terrorista no es necesario

apuntarse en ningún listado, sino que basta con seguir esa base. Por eso son alentados y aparecen a menudo lobos solitarios, delincuentes que actúan por su cuenta o en pequeños grupos y en nombre de la banda. Están siguiendo el sunismo, sin intermediario entre Dios y ellos, solo guiados por las directrices marcadas en el Corán y la interpretación que de él hace Bin Laden, sus sustitutos y sus clérigos. No hay nadie que imponga y tampoco nadie que refrene. El que actúa lo hace por su propia voluntad según la inspiración de la base, con el objetivo final de derrotar a todos los países no islámicos e imponer un gobierno unificado —llamado califato— sobre todos los territorios que alguna vez fueron musulmanes, desde España hasta Indonesia. Esta meta a largo plazo —décadas— se consigue mediante otros pasos intermedios, como derrocar a los gobiernos «impíos», que para ellos son todos los árabes, incluida Arabia Saudí, de donde obtienen buena parte de sus ingresos, y aterrorizar a sus enemigos, los países occidentales —por su apoyo a Israel y su falta de fe— y los socialistas, por su ateísmo y su idea de que todos los hombre son iguales. Bin Laden dijo en 1999 que para ellos «no existen civiles, solo infieles» contra los que es legítimo atentar.

Por su parte, el Estado Islámico, conocido por sus acrónimos en inglés —ISIL o ISIS— y en árabe y forma despreciativa —DAESH, que se puede traducir por «algo que pisar», «intolerante» o «que siembra discordia», según se conjugue—, bajo las mismas ideas, ha decidido afrontar los retos de otra manera. En vez de esperar a sustituir a los gobernantes que no guardan la debida observancia del Islam y luego proclamar el califato, han dado el paso de ejercer el gobierno efectivo sobre las zonas que controlan —grandes áreas de Iraq y Siria— y, desde ahí, comenzar a extenderse. Ese tipo de acción es un choque frontal con su hermana mayor que ha llevado a que sean declarados herejes, tras romper en 2014 todos los lazos que los mantenían unidos. Donde Al Qaeda juega con infiltrar agentes dormidos y mantener a sus dirigentes ocultos, el EI gobierna el territorio, con una administración paralela, fondos propios —en gran medida provenientes del petróleo, obtenido en las zonas que controlan y vendido en el mercado negro— y un gusto excesivo por las ejecuciones públicas de la manera más atroz imaginable. En teoría, el EI permite que cristianos y judíos vivan en su territorio, siempre que paguen el *dhimmi,* el impuesto que las religiones del libro, esto es, aquellas que se rigen por la Biblia, que también es sagrada para los musulmanes, deben para estar a salvo. En la práctica, sin embargo, hay numerosos abusos, con conversiones obligadas so pena de muerte, lo que ocurre con otros credos, como los yazidíes u otros zoroastrianos, que no tienen derecho a optar a esa tasa.

Debido a esa diferente concepción religiosa, ambas ramas tienen una muy distinta concepción de sus necesidades *online*. Hay un fondo común, dado que ambos necesitan conseguir nuevos adeptos entre los musulmanes de cualquier lugar del mundo. Un miembro de Al Qaeda, Abu Amru Al Qa'idy, que se define como seguidor y estudiante de Mustafá Setmarian —fundador de La Base en España y, en

su día, número cuatro de la organización—, recopiló un *Curso en el arte del reclutamiento*, en el que da instrucciones precisas para ello. Una de las más llamativas es la recomendación de no invitar a personas religiosas a unirse a la organización ya que «pueden rechazar el ofrecimiento y ser la causa de tu derrota». El candidato ideal es un musulmán de clase baja, con poca cultura general y en especial en el Corán, que pueda ser manipulado de forma más sencilla. El estudioso puede rebatir con términos teológicos la fanatización y dar al traste con el trabajo de meses o años.

Para cualquier grupo que debe moverse en la clandestinidad, Internet proporciona grandes oportunidades de llegar a grandes masas. Más aún la Red profunda, donde ya hemos visto que es muy difícil —aunque no imposible— rastrear los orígenes de quienes la usan. Una vez en ella, crean foros que actúan como cebo para jóvenes musulmanes radicalizados o tan solo curiosos. En otras ocasiones, se sirven de los ya existentes, cuyos autores no son necesariamente terroristas.

Una vez que la web está en marcha, solo es necesario esperar. La Universidad de Arizona ha llevado a cabo varios estudios donde se demuestra que, cuanto más tiempo pasa en una discusión cualquiera en un sitio yihadista, más radicales y violentos son los mensajes. Una vez que se ha localizado un candidato que presenta las características adecuadas, comienza la lenta labor de adoctrinamiento, en la que tiene un peso específico que el reclutador establezca una relación de amistad —fingida, al menos por su parte— con el futuro combatiente.

Aquí está una de las principales diferencias entre ambas organizaciones. Al Qaeda ha enviado combatientes a luchar, sobre todo, en Afganistán e Iraq, aunque uno de sus objetivos es atentar en los países occidentales, como Estados Unidos, España, Reino Unido, Francia o, en general, aquellos en los que tengan la oportunidad de hacerlo. Estos ataques se llevan a cabo con materiales al alcance de cualquiera, tal vez dinamita de una cantera, un fusil de asalto traído de contrabando desde Bosnia o un curso de vuelo en una academia legal. Para ello, alienta las células durmientes —individuos en apariencia integrados en la sociedad que solo esperan una señal para activarse— y los lobos solitarios. No hay apoyo logístico, no hay ruta de escape, no hay nada más que una reivindicación en vídeo si todo sale bien.

Por otro lado, el Estado Islámico está comprometido en el control del territorio. Para este lo fundamental es conseguir más tropas que mandar allí, sin rechazar que algún lobo solitario sin mucha formación e inspirado por ellos intente cometer una masacre en Europa. También busca enviar mujeres, tanto en su principal función de ser concubinas y —con suerte— esposas de los combatientes, o la secundaria de formar parte de la policía política para controlar la moral femenina y ejecutar a otras de su sexo. Una de las formas de conseguirlo es, de nuevo, a través de Internet. Al contrario que los acólitos de Bin Laden, a menudo, elementos del EI en Siria o Iraq mantienen un contacto directo con sus reclutadores en Occidente. En España hemos tenido varios casos, como, solo en julio de 2015, la mujer detenida en Fuerteventura

con varias niñas en su casa, prestas a acudir a Siria, el hombre arrestado en Melilla que grababa vídeos exaltando la *yihad* o el marroquí atrapado en Badalona que mantenía múltiples perfiles en redes sociales desde donde lanzaba consignas a favor del terrorismo y, de paso, tanteaba la afinidad de los que le seguían con vistas a poder enviarlos en el futuro a Oriente Medio.

Estos capturados son el penúltimo eslabón de la cadena y son muy vulnerables. No solo su actividad *online* es visible y rastreable, sino que, a menudo, deben contactar en persona con los radicalizados a los que han de reclutar y enviar, con el elevado riesgo de que estén vigilados por la policía. Los grupos que se ocupan de trasladarlos luego desde Turquía u otros países a los frentes de batalla son más valiosos para la organización, como los ideólogos y contactos. Por ello toman medidas especiales. A menudo los arrestados no saben nada de sus intermediarios. Ni un teléfono móvil ni una dirección de correo. ¿Cómo es posible?

Por un lado está el uso de la Red profunda, que permite un anonimato bastante eficiente. A eso se suma el uso de programas de encriptación como *Asrar al-Mujahedeen* (Secretos Muyahidines) que protege con uno de varios algoritmos de alta seguridad, a elegir, los mensajes que se intercambian. Es una aplicación sencilla, creada por voluntarios, que se puede descargar con facilidad de Internet. No incluye ninguna novedad. Todos los sistemas de cifrado que implementa ya existen y son bien conocidos, tan solo los han unido, algo al alcance de cualquier programador de nivel medio. Aun así, cumple su propósito con nota. En criptografía se considera un algoritmo bueno, no aquel que es secreto, sino el que, siendo conocido por la comunidad científica, ha sido puesto a prueba y no se puede derrotar con facilidad. Toda encriptación es vulnerable, tan solo es un asunto de tiempo saber cuántos ordenadores tienen que estar trabajando a la vez para *reventarlo*. Si hace falta toda la capacidad de computación disponible durante meses o años, es que el mensaje es seguro. Cuando se logre interpretar, habrá perdido toda la importancia que pudiera tener. Hoy no es cuestión solo de contraseñas más o menos complejas. Para poder descifrar el contenido hace falta un doble sistema conocido como criptografía asimétrica, del que hablaremos en el capítulo siete. En resumidas cuentas, eso quiere decir que cada mensaje solo puede leerlo su destinatario, único y concreto. Aunque lo encuentre cualquier otro, ninguna clave funcionará.

Hemos visto, pues, que las organizaciones terroristas de inspiración islámica utilizan la Red, sobre todo, como medio de propaganda y reclutamiento. ¿Tienen capacidad de algo más? ¿Pueden llevar a cabo un ataque del tipo *Stuxnet* o peor contra los países occidentales? Ese temor es habitual entre los gobiernos implicados, si bien los estudios parecen concluir que es muy improbable.

Como hemos comentado más arriba, el ejercicio *Digital Pearl Harbor* del año 2002 calculó que harían falta al menos doscientos millones de dólares y cinco años de preparación para poder llevarlo a cabo. Eso contando con un grupo multidisciplinar dedicado a ello en exclusiva y sin sufrir interferencias externas. Las células terroristas

están acosadas, dentro y fuera de sus fronteras. En las zonas dominadas por el DAESH sufren continuos bombardeos aéreos de los aliados occidentales, contraataques de los gobiernos sirio o iraquí y la feroz oposición de kurdos y chiíes, a menudo sufragados por Irán. En el exterior, la vida media de una célula operativa, aunque sea de apoyo, es de pocos meses en el mejor de los casos, antes de ser detenidos. Además, es difícil suponer que vayan a disponer de los especialistas que necesitan en múltiples disciplinas. Recordemos lo que hemos dicho más arriba: el caldo de cultivo ideal lo encuentran entre la gente con menos formación, con las debidas excepciones. Hallar tantas piezas y ponerlas juntas es casi imposible.

En los foros yihadistas se fantasea a menudo con grandes acciones, como la destrucción de una planta nuclear o química o el sabotaje sistemático de la red financiera de un país, pero, hasta ahora, los ataques que se han llevado a cabo han sido más parecidos a lo que cualquier grupo de chavales con conocimientos en informática puede hacer desde su casa. Han consistido, casi en exclusiva, en el tipo «B», en su variedad de denegación de servicio y sustitución de la información presente por otra.

Poco después del atentado contra el semanario satírico francés *Charlie Hebdo*, el ubicuo movimiento Anonymous, del que hablaremos en el capítulo diez de este libro, lanzó una fútil «declaración de guerra» al Estado Islámico y a aquellos que lo apoyasen. Como respuesta a esto y a la reacción popular en todo Occidente bajo la frase *Je suis Charlie*, el grupo AnonGhost, de inspiración palestina, atacó varias páginas web francesas y sustituyó los mensajes por proclamas musulmanas e imágenes *ad hoc*.

AnonGhost está formado por un número indeterminado de personas repartidas por diferentes países, cuyas acciones tradicionales han sido antisionistas y, en menor medida, antioccidentales. A partir de 2015 han apoyado sin ambages al EI. Sus actividades se han limitado, como los grupos *amateurs* patrocinados por Rusia o Serbia que hemos visto antes, a acciones muy sencillas y muy similares a las de sus rivales de Anonymous. Las más llamativas, cuatro ataques a otras tantas webs de agencias policiales locales en los Estados Unidos, a las que cambiaron la página de presentación por mensajes como «Dejad de matar musulmanes» o «Muerte a Israel. Viva Hamas». Su mayor logro fue introducirse en una página de baja seguridad de la Casa Blanca en la que colgaron un alegato con las soflamas habituales.

No hay que entender este grupo como una red organizada, sino como varios conjuntos variopintos de personas que actúan según su disponibilidad y en los que no hay una voz unánime. Según evolucionen las tendencias, unos nuevos se unen y otros dejan de pertenecer —por el sencillo método de no conectarse más a sus chats—. Jamás se han visto entre sí y ni siquiera se conocen las caras, una manera muy típica de relacionarse en la era de Internet no solo los ilegales, sino cualquier grupo con aficiones comunes.

Otra banda, llamada Team System DZ, realizó ataques similares en Francia el día

19 de enero de 2015. Estos tuvieron repercusión en España porque se vieron afectadas hasta cuarenta páginas de ayuntamientos de Navarra. No habían sido el objetivo, sino la empresa que les proporcionaba alojamiento web y que estaba situada en el país vecino.

Uno de los ataques más serios ocurrió contra la televisión francesa TV5 Monde a principios de abril del mismo año. Fue de tal magnitud que perdieron la capacidad de emitir en directo, teniendo que limitarse a reposiciones. También tomaron control de la página web y de las cuentas de la cadena en Twitter y Facebook. Como es habitual, colgaron mensajes a favor del Estado Islámico… y eso fue todo. La investigación posterior demostró que los responsables de la cadena habían caído en uno de los trucos más viejos del oficio, el de la ingeniería social. Más fácil que conseguir el acceso a un sistema informático es que alguien de los que trabaja allí te dé la contraseña. Para ello enviaron correos electrónicos que simulaban pertenecer al servicio técnico. En ellos se simulaba que había habido una desconexión del sistema y que se debían introducir de nuevo las contraseñas. Uno de los empleados que lo recibió picó en el anzuelo. Desde ese momento, sin ninguna inversión de tiempo ni dinero, los atacantes pudieron hacerse con el control absoluto de los ordenadores y redes del canal. Algo similar realizan los delincuentes que intentan robar cuentas bancarias, como veremos en el capítulo seis, en la técnica denominada *phishing*.

Desearían realizar otro tipo de acciones que encajaran más en la ciberguerra, algo que hasta ahora parece fuera de su alcance. Encuentran problemas similares al uso de armas biológicas, químicas o *bombas sucias* que vuelvan inhabitable un área determinada por contaminación radiológica. La logística y conocimientos necesarios no son sencillos en absoluto para grupúsculos pequeños, de formación escasa en tan peligrosas artes y siempre acosados por sus enemigos.

La lucha contra el terrorismo también tiene un importante factor en la *deep web*, en el que los dobles agentes y la desinformación funcionan con libertad. La policía de los diferentes países cuya legislación lo permite intenta hacerse pasar por radicales para penetrar las redes —que ya sabemos que son compartimentadas al máximo por la propia naturaleza de las organizaciones—. Incluso se va más allá. Es habitual encontrar manuales de explosivos en las páginas yihadistas. Algunos de estos han sido preparados por los servicios de inteligencia de manera que, si alguien sigue sus instrucciones para preparar bombas, detonarán en el momento de hacer la mezcla de productos químicos. Es siempre muy arriesgado intentar acciones peligrosas sin tener la formación adecuada para hacerlo y un manual bajado de Internet no la sustituye.

4

LA MUERTE RETRANSMITIDA

Carme Ann Álvarez se aparta un mechón de la cara mientras habla con el director de la prisión de Cagayan de Oro en la que está internada, al norte de Mindanao, la más oriental de las islas Filipinas. Apenas tiene dieciocho años, los ojos grandes y oscuros, nariz chata y cejas rectas. Lleva unos muy discretos pendientes en las orejas, una concesión sobre su uniforme de presidiaria: una camiseta amarilla en que se puede leer su condición en grandes letras negras, y un pantalón oscuro. Poco después de esa entrevista recogería su media melena en trencitas, al estilo tropical. Entiende por qué está encerrada, pendiente de juicio, pero como no ha conocido otra vida, no ve motivos para callar como lo hacen otros miembros de la trama.

No se le puede llamar afortunada. Prostituta desde antes de la adolescencia, una niña de la calle sin recursos ni sitio alguno al que acudir, había conocido lo peor de la sociedad antes de que la mayoría de las personas saliese de entre los algodones familiares. Tenía trece y muchas noches dormía a la intemperie cuando en 2011 El Americano se le acercó y le ofreció dinero y un techo, al menos temporal. Carme, que se hacía llamar Ángel, no se llamaba a engaño. Incluso las personas que parecían bondadosas solo buscaban su cuerpo. Este hombre, alto, muy delgado, que fumaba sin parar, tenía algo terrible en sus ojos. Y no era para menos. No se conformó con abusar de ella de todas las formas imaginables, muchas de las cuales incluían dolor, sino que además, lo grababa con diversas cámaras y lo retransmitía por Internet. Decía que cobraba por ello y, visto el tren de vida que tenía, la chiquilla lo creía. Siguió con él, no por amor, sino por los beneficios. Aunque a veces la llamase novia. También lo hacía con Lovely, otra mujer algo mayor que también compartía la casa en la que vivían. Y las niñas. Las niñas eran lo peor. Las mayores no pasaban de los trece años. No quiere recordar lo que llegó a pasar con algunas…

Al cumplir los diecisiete, El Americano perdió interés en su cuerpo ya casi maduro. Por eso empezó a tener un trabajo diferente. Debía buscar por las calles niñas pequeñas que estuvieran solas y llevárselas a su novio. En las atestadas calles de la zona más pobre de Cagayán era fácil. A cambio de un bocadillo o algo que comer en algún puesto de la zona, las chiquillas la acompañaban con facilidad. Luego, en manos del forastero, eran sometidas a abominaciones sin nombre por encargo… hasta que en una de esas se les fue la mano. Las exigencias del «cliente» que miraba la webcam eran tan extremas que una niña murió. Y no pasó nada. Siguió sin pasar hasta que, en un descuido, dos pequeñas primas se escaparon. Cuando la policía llegó, fue en parte un alivio. Estar en la cárcel no es tan malo, después de todo.

LA BANALIZACIÓN DEL SUFRIMIENTO

La muerte es algo presente en nuestro día a día. Como dice el viejo adagio «ninguno nos vamos a quedar aquí para contarlo». Es uno de los misterios metafísicos que ha preocupado a la humanidad desde sus albores. Los ritos funerarios y los enterramientos son habituales desde incluso antes de la llegada del actual *Homo sapiens*. Lo que hay después de la muerte ha sido una de las principales preocupaciones de la religión y aun del hombre moderno. El propio trance fascina y aterra en la misma proporción. En cualquier caso, es difícil ver morir a una persona, mucho más en condiciones violentas. Hoy vivimos en un mundo rodeado de cámaras. Casi cada persona lleva un potente grabador de imágenes en el bolsillo, hay sistemas de vigilancia en las calles y también en los interiores, los medios de comunicación están cercanos a la noticia. En resumen, es fácil captar un accidente mortal o un acto de guerra que luego van a ser retransmitidos hasta la saciedad por los noticieros más sensacionalistas.

Según las teorías más importantes, uno de los rasgos característicos de la psicopatía es la ausencia de empatía. Es decir, el psicópata es incapaz de considerar a la otra parte como su igual, como alguien *real* y, por tanto, su sufrimiento no le afecta. A una persona que no tiene esa condición, la tortura o la muerte de otro, incluso de animales, le causa malestar y congoja, por una circunstancia denominada *proyección*, esto es, el hecho de sentirnos reflejados en la parte doliente. No obstante, la desensibilización se puede aprender, la sensibilidad se puede anestesiar, a base de exponerse a esas situaciones. Por eso, los miembros de los servicios de emergencia —policía, bomberos, médicos, personal de ambulancias— suelen conseguir alta puntuación en el test de Robert Hare, una serie de pruebas desarrolladas por ese psiquiatra norteamericano para detectar la insensibilización. Por tanto, el bombardeo diario de muertes horribles puede hacer que el ciudadano medio se impresione menos por ello.

En el mundo de la telecomunicación y la inmediatez proliferan las páginas web dedicadas a sectores muy específicos de la población. Igual que el porno se ha especializado en cada parafilia conocida, lo mismo ha ocurrido con otros sectores del ocio… entre ellos, el de la muerte. La muerte de otros, se entiende. Las páginas dedicadas a mostrar el lado más crudo del día a día surgieron en cantidad en la primera mitad del nuevo milenio, hasta el punto de recibir un nombre para el género, *shock site* (sitio ofensivo, en inglés). Algunas, como *Rotten.com*, siguen en activo hasta hoy. Otras, como la *Ogrish.com* original, fueron vendidas a terceros.

La primera de las mencionadas, cuya traducción es «podrido», fue la pionera. Fundada en 1996, su estructura ha cambiado muy poco con los años, hasta el punto de que hoy parece una reliquia de tiempos pasados. En la parte superior presenta el dibujo de un esqueleto animado saliendo del sudario junto al título de la web y la frase, en inglés, «Cuando el infierno esté lleno, los muertos caminarán sobre la

Tierra». Debajo, en rojo, se puede leer, siempre en el mismo idioma, «Maldad pura desde 1996» y en una tipografía más pequeña, «Ruborícese, por favor». Después, una serie de hipervínculos colocados sucesivamente, cada uno de los cuales da acceso a fotografías de algún resto humano. En la actualidad y desde hace cuatro años, el primer enlace lleva a una mano amputada y el segundo a un vagabundo, vivo, cuya pierna izquierda está consumida por una infestación de gusanos. Apenas hay información al respecto. No se explican los motivos ni las soluciones. Como mucho, algún comentario, como el del último caso descrito, que, bajo el título «Agusanado», dice: «¿Qué puede llevar a un hombre a tener esta condición?». El único objetivo de la web es causar impresión y hasta náusea. Desde el año 2012 el sitio apenas tiene movimiento, pero continúa *online*. Sus imágenes son utilizadas una y otra vez por particulares que desean causar ese mismo efecto en las redes sociales. La diferencia es que quien entra a Rotten ya sabe lo que le espera, mientras que en Twitter se sorprende al incauto, que reacciona con desagrado y, a menudo, con denuncias que no pueden llegar a ningún sitio, porque el delito no existe.

Al año siguiente, en 1997, el holandés Dan Klinker creó una segunda página, *Ogrish.com*, alojada en los Estados Unidos, que se puede traducir como «Relativo a los ogros». Presentaba una estética más elaborada, con un fondo negro y el título enmarcado por unas manos ensangrentadas. En su última etapa cambió a un diseño más amable, en blanco y con menos gráficos, por lo que tardaba menos tiempo en *cargar* en un ordenador doméstico. El principal color de la web era el rojo oscuro y, como novedad respecto a la anterior, alojaba vídeos además de fotografías. Proporcionaba más información que su antecesora, a menudo unas pocas líneas, en ocasiones reportajes enteros. Llegó a tener a cinco empleados a tiempo completo, además de una cantidad indeterminada de reporteros por cuenta propia que vendían lo que encontraban, desde accidentes hasta asesinatos. Por ello siempre se ha sospechado que gran parte de estos *periodistas voluntarios* eran miembros de los servicios de emergencia. La web se mantenía con publicidad y con los ingresos que proporcionaba la parte privada de la misma, a la que solo se podía acceder tras pagar por registrarse en ella. Los trabajadores, tanto los fijos como los *freelance*, no se conocían entre sí y residían en diferentes lugares del mundo. Ni siquiera podían ponerle rostro al fundador, esquivo no solo para la prensa y las autoridades, sino hasta para sus propios compañeros.

Empezó mostrando tragedias locales, pero con la guerra de Iraq, a partir del 2001 amplió su catálogo a las decapitaciones islamistas y otras barbaridades. Para ello llegaron a desarrollar unas arañas, parecidas a las que vimos en el capítulo uno, para rastrear páginas yihadistas en busca de otros contenidos similares. Según sus propias estadísticas, hasta un treinta por ciento de sus visitantes eran mujeres y casi la totalidad la utilizaban como fuente de información alternativa, no como aspersor de morbo. Sin embargo, mezcladas con las imágenes crudas había anuncios de sitios pornográficos, incluso enlaces directos a escenas equis. Eso es un indicio de que su

naturaleza tal vez fuera mucho más retorcida.

Desde el principio estuvo sumido en la polémica, debido a que solía exponer imágenes de víctimas sin su consentimiento (cuando estaban vivas) ni de sus familiares, como hizo con las del huracán *Katrina* que asoló Nueva Orleans en 2002. El año anterior ya había entrado en la infamia al mostrar las fotografías de los ciudadanos que, durante el ataque a las Torres Gemelas de Nueva York, decidieron saltar al vacío en vez de enfrentarse a las llamas que las devoraban tras la colisión de los dos aviones. La prensa estadounidense había decidido no publicarlas. Debido a esta exposición en Ogrish, su autocensura no sirvió de nada y no tardaron en aparecer vergonzantes montajes en los que se hacía burla de los fallecidos.

Las decapitaciones de extranjeros en Iraq alimentaron sus páginas durante los siguientes meses. Tras mostrar el vídeo en que se podía ver la del misionero surcoreano Kim Sun-Il en 2004, *hackers* de aquella nacionalidad atacaron el servidor, dejándolo sin servicio durante un tiempo.

En 2005, un grupo de protección de la infancia alemán encontró un resquicio por el que limitar sus actividades. La legislación exigía a cualquier página que ofreciera contenidos para adultos una verificación de edad, para evitar que los menores accedieran. Como no era el caso, la justicia ordenó el corte del acceso al sitio, para lo cual se bloqueó la IP que utilizaba desde los proveedores de servicios de Internet. Uno de ellos Level3, ubicado en Frankfurt, daba servicio a los Países Bajos, Francia, Polonia, Italia y Suiza. Todos esos países también se quedaron sin poder verla.

Al final, en noviembre de 2006 la página se integró en otra, que hasta hoy continúa funcionando, LiveLeak —algo así como «goteo de vida»—, que había sido fundada un mes antes por el mismo equipo de Ogrish, con pretensiones de sitio de noticias y una enorme cantidad de vídeos que hace difícil encontrar los contenidos más repugnantes, que, de hecho, solo están disponibles para aquellos que se registran en la web. De esta manera ha conseguido una cierta legitimación que no tenía su predecesora, aunque, como aquella, ha rechazado retirar esos contenidos cuando se le ha solicitado. En palabras de su cofundador, Hayden Hewitt: «Esto está pasando, es la vida de verdad, vamos a mostrarlo». LiveLeak afirma que colabora con la justicia; si quien sube las imágenes —homicidios, incendios, etc.— es el responsable de hacerlas, entregará los datos de los que disponga a las autoridades correspondientes. Sin embargo esto no siempre ha sido así y Ogrish no ha contestado a las requisitorias, por ejemplo, de la Audiencia Nacional de España.

Y es que nuestro país había vetado el acceso a la página un año antes que Alemania, aunque aquellos con unos ciertos conocimientos de informática se podían saltar la prohibición de una forma más o menos fácil.

El 11 de marzo de 2004, entre las 7.36 y las 7.40 de la mañana, unos terroristas islamistas detonaron diez mochilas-bomba —más tres que fallaron y fueron recuperadas por la policía— en cuatro trenes de cercanías de Madrid, todos ellos con destino final en la estación de Atocha. Asesinaron a ciento noventa y dos personas e

hirieron a casi dos mil. Desde el momento en que se supo del ataque, centenares de miembros de los servicios de emergencia acudieron a ayudar, hasta que el centro de coordinación impidió que acudiera más gente. La ciudad es muy grande y hacía falta que siguiera atendida.

El 22 de octubre de ese mismo año, en *Ogrish.com* apareció una serie de treinta y cuatro fotografías «exclusivas», muy gráficas, con restos de los fallecidos. Torsos desmembrados o carbonizados, cabezas guardadas en cajas de cartón y un largo catálogo del horror que se vivió aquel día. El juez de la Audiencia Nacional instructor del sumario del 11-M, Juan del Olmo, contactó con la Brigada de Investigación Tecnológica de la Policía Nacional, a la que ordenó que esclareciera los hechos.

A requerimiento de esta, emitió un auto solicitando a Ogrish que retirase de manera inmediata esos contenidos y que le remitiese los datos disponibles sobre quien se las había entregado. La página se negó, amparándose en que mostrar tales horrores no violentaba la legislación de Holanda ni de Estados Unidos. En sentido estricto, tampoco la española. Mostrar cadáveres no es delictivo, todo lo más un ilícito civil —pecuniario y de obligación de eliminar las fotos— que pueden reclamar los familiares en un proceso largo, costoso y no siempre triunfante. Sin embargo, como por aquel entonces el sumario estaba declarado secreto, esas imágenes estaban, de hecho, violando la disposición judicial y su publicación se entendió como una obstrucción a la justicia. Así, pues, mientras la BIT se lanzaba a la investigación, el magistrado ordenó, como ya hemos visto, que se clausurase el acceso a la web desde España, de lo que también se encargó la policía, que contactó con cada una de las empresas que proporcionaba servicio directo de Internet en el país, y establecieron medidas para impedir su visualización. De este modo, solo utilizando *proxies* situados en el extranjero podría un nacional acceder a los contenidos vedados. Una medida, en principio tan polémica que podría entenderse como censura por algunas organizaciones, fue aplaudida incluso por la siempre crítica Asociación de Internautas, cuyo presidente, Víctor Domingo, afirmó a la agencia EFE que Ogrish respondía solo a la «satisfacción morbosa» del espectador.

Los especialistas de la BIT, mientras tanto, estaban trabajando. Partían de la base de que quien había realizado esas imágenes debía estar autorizado para pasearse por el lugar, dado que se veían bomberos, policías y sanitarios y nadie reparaba en el cámara, algo extraño de haber sido un civil sin permiso. Realizaron un pormenorizado estudio del contenido de aquella web, que, como es obvio, supuso una prueba difícil, dada la naturaleza de lo que en ella se mostraba. Encontraron otra serie de fotografías originadas en España. Habían sido tomadas en un accidente de tráfico. La pasajera, una niña, había impactado con el guardarriel y resultó decapitada y con el brazo izquierdo amputado. Las imágenes mostraban la cabeza en la cuneta y el miembro seccionado en el asfalto, así como el turismo volcado y un camión de bomberos madrileño; el cuerpo aparecía cubierto por una sábana blanca que era levantada para realizar la instantánea.

Cada cámara tiene unos datos únicos, llamados EXIF que, aunque no son visibles para el usuario medio, pueden ser consultados con los programas adecuados, a los que recurrieron los agentes. Descubrieron que tanto las escenas del 11-M como esta habían sido retratadas con la misma máquina, una Ricoh Caplio G3. Respecto a las primeras, se supo que habían sido grabadas en dos entornos diferentes. El primero, entre las 12.58 y las 13.19, en la estación de El Pozo, y el segundo, entre las 16.28 y las 18.01 en la calle Téllez.

El siguiente paso, una vez determinado el accidente, fue hablar con los servicios de emergencias de toda la Comunidad Autónoma para averiguar qué dotaciones habían estado en esa carretera y comparar la relación con el listado de aquellos presentes en Atocha. Solo una ambulancia, subcontratada por el Servicio Madrileño de Salud, había estado presente en los tres lugares y en las horas precisas. Cuando la BIT se lo comunicó al juez, este ordenó la inmediata detención de los responsables por un delito de revelación de secretos, al asimilarlos a funcionarios públicos con la obligación de guardarlos.

Así, pues, el 28 de octubre, tan solo una semana después de iniciado, el caso había quedado esclarecido. Se detuvo a tres personas, entre los veintiocho y los treinta y dos años, que reconocieron su participación en los hechos. El primero era conductor de ambulancia y autor de las fotografías del accidente y parte de las del atentado. El segundo, personal de otro vehículo similar, había realizado el resto de las imágenes. El último compartía con los otros dos las imágenes realizadas. El tercero era víctima del conocido como «síndrome de emergencias», por el que siempre intentaban llegar los primeros a las escenas más escabrosas, no solo para hacer su trabajo, sino también para conseguir esas imágenes impactantes que luego utilizaban en la formación de los novatos que querían acceder al servicio. Querían prepararles ante los horrores que iban a ver. Sin embargo, su actitud ya había pasado de lo educativo a lo morboso. Cuando decidieron enviar a Ogrish sus *tesoros*, traspasaron la línea. Hoy, todos esos horrores son aún visibles en Internet con una sencilla búsqueda.

Aunque la página en cuestión no pertenecía a la Internet profunda, debido a su falta de colaboración toda la investigación se llevó a cabo como si así fuese, agudizando el instinto policial y sin poder recurrir a las direcciones IP que facilitan la labor de ubicación del autor de los hechos.

Esas páginas siguen existiendo. Algunas se especializan como Mundonarco y sus derivadas, que muestran las barbaridades que se están cometiendo hoy en día en México en la lucha entre bandas de crimen organizado. Son habituales los vídeos de interrogatorios y ejecuciones entre los Zetas, los Caballeros Templarios y el Cártel del Golfo. A menudo se realizan con cuchillos, hachas o machetes y las decapitaciones o desmembramientos son las imágenes favoritas. En el país azteca, quienes difunden esos vídeos se juegan la vida por el hecho de hacerlo, ya que ese tipo de «mensajes» está destinado al rival, no a que el gran público conozca la verdad

que hay detrás del oropel de los grandes capos.

La exposición continua a la grabación de la muerte de personas, muy a menudo de manera lenta y cruel, tiene un importante efecto de insensibilización sobre el ser humano. Esto es incluso más peligroso para los niños, que están en una fase muy influenciable de su vida. Si desconectamos nuestra empatía, nuestra capacidad de ponernos en el lugar de los demás, del torturado o asesinado, estamos un paso más cerca, no solo de no ayudar al prójimo, sino de causarle nosotros el sufrimiento.

EL MITO DE LAS PELÍCULAS *SNUFF*

En 1996, el director español Alejandro Amenábar rodó *Tesis*, su ópera prima. Giraba alrededor de las conocidas como películas *snuff*, la misma inspiración que serviría tres años más tarde para la estadounidense *Asesinato en ocho milímetros*. El tema no era nuevo. En 1969 fue asesinada la actriz Sharon Tate, esposa del director de cine Roman Polanski, junto a otras cuatro personas, a las que seguirían tres más en diferentes localizaciones de California. Todas estas muertes fueron cometidas por una secta conocida como la Familia Manson, cuyo líder era Charles Manson, conocido criminal y psicópata que se encuentra cumpliendo condena a perpetuidad por estos asesinatos. Dos años más tarde, Ed Sanders publicaría un libro sobre estos hechos y sus protagonistas, donde mencionaría por primera vez la palabra *snuff*, que se haría famosa en 1976 gracias al film homónimo que se pretendió vender en un principio como real, recurriendo al mismo truco de *Holocausto caníbal* o la más reciente *El proyecto de la bruja de Blair*.

Así, pues, nos encontramos ante un fenómeno que ha calado en el acervo popular y que podemos definir como *grabación en la que el protagonista es asesinado con el único propósito de obtener beneficio económico con la venta de la cinta*. Como hemos visto, grabaciones de muertes existen y son hasta habituales en los informativos de la televisión. Uno de los más populares fue el fallecimiento de la pequeña de trece años Omayra Sánchez Garzón en Colombia, en 1985, cuando la erupción del volcán Nevado del Ruiz provocó el deshielo de una gran masa de agua que arrasó el cercano pueblo de Armero. Había quedado atrapada bajo los restos de su casa y lo único que asomaba fuera del fango era la cabeza. Solo había dos formas de liberarla, amputarle las piernas o utilizar una motobomba para desaguar las ruinas. Ambos medios estaban fuera del alcance de los rescatadores y durante tres días las televisiones del mundo entero retransmitieron su lenta agonía hasta que falleció de gangrena gaseosa el 16 de noviembre. En los años noventa se vendían bajo el título *snuff* VHS con contenidos similares, que incluían ese y otros casos, como fusilamientos, suicidios, ahorcamientos y electrocuciones, incluida la del anarquista Leon Czolgosz, asesino del presidente McKinley, el primer año del siglo pasado, realizada por el ínclito Thomas A. Edison, al igual que *Electrocución de un elefante*

(que utilizó como arma publicitaria contra la competencia). Destacó la serie de cinco películas del estadounidense Damon Fox *Traces of Death* (*Las huellas de la muerte*), iniciada en 1993, que mostraba los fallecimientos en toda su crudeza, como más tarde haría la web *Ogrish.com* de la que hemos hablado en el apartado anterior. Entre ellos estaba el suicidio en 1987 del político estadounidense Budd Dwyer, que se disparó en la cabeza durante una rueda de prensa, el accidente del actor Vic Morrow y dos niños, a los que les cayó encima un helicóptero durante el rodaje en 1982 de la película *En los límites de la realidad*, de Steven Spielberg; el bombardeo del mercado de Sarajevo durante la guerra de Bosnia de 1994, que mató a más de sesenta personas y varias escenas de niños muertos en diversas situaciones. Desde la segunda parte, las películas son acompañadas de música de estilos *death metal* y *grindcore*, de baja calidad. Fue prohibida en Reino Unido, donde se declaró que carecía de todo valor «periodístico, educacional o contexto alguno que justificase las imágenes mostradas». Según la definición que hemos dado más arriba, ninguna de esas filmaciones se puede considerar *snuff*, puesto que la intención de las muertes nunca fue la venta de las mismas.

Como hemos dicho, con la popularización de los teléfonos móviles, todo el mundo dispone de una poderosa cámara con la que registrar cualquier hecho. Eso facilita que se pueda inmortalizar el fallecimiento de personas y, con la llegada de Internet, que sea compartido después con una facilidad asombrosa. Más aún, la Red permite el contacto de individuos con gustos similares, por extraños o retorcidos que sean, como el foro, hoy desaparecido, *The Cannibal Cafe (El Café Caníbal)*, al que acudían personas que tenían interés en devorar a otras o, más peculiar aún, ser comidos por otro humano. La web era un ejemplo de Internet profunda convencional. Si bien no hacía falta nada especial para acceder, no aparecía en los buscadores, por lo que era difícil de encontrar sin la ayuda de un tercero. Se alojaba dentro de un lugar llamado *Necrobabes.org*, que se podría traducir por «necrochicas» o chicas muertas, que alojaba diferentes recursos sobre el tema, desde los cómics de ginecofagia —que mostraban cómo cocinaban y comían mujeres— de Dolcett hasta fotos que fingían de manera torpe hechos similares. En un subdirectorio asignado a alguien que se hacía llamar *Perroloco* estaba ese refugio para antropófagos en el que se movía un ingeniero berlinés de cuarenta y tres años, Bernd Jürgen Armando Brandes, deseoso de entregar su cuerpo de la manera más literal. Así, contactó con otro alemán, Armin Meiwes, de cuarenta y uno, que acabaría por ser conocido como *el Caníbal de Rotenburgo*. Este había quedado ya en su domicilio particular con otros cuatro hombres que respondieron a sus anuncios para ser devorados en otras tantas ocasiones. Después de una charla amistosa, los dejó marchar a todos. Habían manifestado dudas y él no quería forzar en lo más mínimo a su víctima. Con Bernd fue diferente, dado que mostró una absoluta seguridad sobre lo que quería y lo que iba a pasar. Por eso, tras hacerle ingerir grandes cantidades de drogas y alcohol, Meiwes empezó por cortarle el pene —los deseos de la víctima incluían que se lo

arrancara a mordiscos, pero fue imposible de realizar, por lo que usó un cuchillo— y dárselo a probar. Como resultó demasiado difícil de comer crudo, lo cocinó con sal, pimienta, vino y ajo, utilizando como aceite parte de la grasa corporal del ingeniero. Se quemó hasta ser incomestible, por lo que acabó cortándolo en trocitos y dándoselo a su perro. Después de aquello, dejó que Brandes se desangrara durante tres horas antes de degollarlo y colgarlo de un gancho de carnicero en una habitación-matadero que había adaptado a tal efecto en su pequeño apartamento. Grabó todo el proceso en una cinta de dos horas de duración, que, no obstante, no hizo nunca pública —por lo que tampoco se puede considerar *snuff*—. Durante los siguientes meses, consumió hasta veinte kilos de la carne, que guardaba en un congelador bajo cajas de *pizza*, hasta que un estudiante de Innsbruck denunció a la policía nuevos anuncios en los que buscaba otra persona a la que matar y comer. Fue detenido en diciembre de 2002 y condenado en primera instancia a ocho años de prisión. La revisión del caso, sin embargo, convirtió la sentencia en cadena perpetua, que se encuentra cumpliendo en la actualidad. Algunas personas estiman que la grabación obtendría un valor de hasta cincuenta mil euros en el mercado negro, si bien es algo demasiado abierto a la interpretación. En cualquier caso, es muy improbable que alguna vez vea la luz.

Un *daño colateral* de todo este asunto fue el cierre en 2004 de The Cannibal Cafe, que desapareció sin dejar rastro. Su matriz, Necrobabes, aguantó diez años más. Hoy, ninguna de las dos páginas existe, si bien tienen su reflejo en diversos sitios alojados en TOR.

Otros que grabaron sus atrocidades fueron los jóvenes ucranianos conocidos como *Los Maniacos de Dnepropetrovsk*. En 2008 apareció en los lugares más oscuros de Internet un vídeo llamado *3 guys & 1 hammer* (tres tipos y un martillo). Homenajeaba con el título a otra grabación más *inocente* aunque muy desagradable llamada *2 girls & 1 cup* (dos chicas y una copa), que era el muy gráfico tráiler publicitario de un película sobre coprofagia; llegó a alcanzar tal fama que incluso en la televisiva *Padre de familia* hay una escena que la recrea. Esta segunda filmación, sin embargo, era mucho más abyecta y terrible. Comienza con un varón de mediana edad tirado en el suelo, semiinconsciente, que sostiene un objeto pesado sobre su estómago. A los pocos segundos, se lo quita de encima con esfuerzo. Acto seguido, aparece en el encuadre un joven cuyo rostro no se ve, que porta un martillo envuelto en una bolsa de plástico. Sin dudar y sin mediar palabra, le golpea el rostro de manera salvaje. Después del brutal ataque, le clava un destornillador en el ojo y más tarde en el abdomen. Por fin vuelve a golpearle con el martillo en la cabeza para asegurarse de que está muerto. Durante el vídeo, uno de los dos asesinos sonríe a la cámara y se mofa del occiso. Después caminan de vuelta a un turismo negro aparcado en la cercana carretera y comentan con calma lo que acaban de hacer. Se sorprenden de que siguiera respirando después de hurgar con el destornillador en su cerebro desnudo. Acaban riéndose mientras se lavan las manos con una botella de agua.

La víctima era Sergei Yatzenko, un hombre de cuarenta y ocho años que residía

en el pequeño pueblo de Taroms'ke, en Ucrania. Se encontraba jubilado por un cáncer de garganta, pero se negaba a considerarse inútil, por lo que realizaba pequeños trabajos domésticos allí donde se le requería. Tenía dos hijos y un nieto, y se hacía cargo de su madre, discapacitada. El 12 de julio de 2007 se había marchado de casa en su motocicleta para repostarla y después visitar al pequeño. Para ello tenía que pasar por un área deshabitada, de donde nunca salió. Fue hallado cuatro días después, con la cabeza destrozada y ya en estado de descomposición.

Las andanzas del par no duraron mucho más, ya que el 23 de julio fueron arrestados cuando intentaban vender el teléfono móvil de otra de sus víctimas. El dependiente les pidió que lo encendieran para ver si funcionaba y, al hacerlo, las autoridades pudieron triangular su posición. Uno de los asesinos, junto a un encubridor, fue arrestado al lado de la caja registradora y el segundo poco después en su domicilio. Se llamaban Viktor Sayenko e Igor Suprunyuck, ambos de diecinueve años, amigos desde que empezaron a ir al colegio.

Aquel del martillo no había sido su primer crimen, sino ¡el undécimo! Todavía asesinarían a otras diez personas en una loca carrera hacia ninguna parte que habían comenzado el 25 de junio. Veintiuna personas asesinadas en menos de un mes.

El vídeo del homicidio fue exhibido durante el juicio oral, en la audiencia pública que tuvo lugar el 29 de octubre de 2008, para horror de la concurrencia. En diciembre de ese mismo año, llegó a Internet, donde todavía está presente hoy, ya sin necesidad de una búsqueda exhaustiva.

La novia de uno de los acusados, condenados a cadena perpetua —el encubridor, Alexander Hanzha, cumple nueve años por varios atracos anteriores—, afirmó que los dos chicos estaban produciendo un total de cuarenta vídeos *snuff* por encargo de un desconocido millonario dueño de un sitio de la *deep web*. La hipótesis se descartó durante el juicio porque no se encontró ni un indicio de ello, a pesar de que el abundante material informático que se les incautó fue estudiado en profundidad y no hacían esfuerzos por esconder sus fechorías. También había grabaciones de la mayoría de las otras muertes que causaron, hasta de animales. En uno de estos casos, crucifican a un gato al que luego disparan con balines y amordazan porque les molestaban sus maullidos.

El recurso a un indemostrable contrato para hacer vídeos *snuff* es habitual en esta clase de homicidios causados por psicópatas de manual, como una forma de buscar una explicación a lo que no la tiene en nada más allá de la maldad humana. Con los trágicos asesinatos de las niñas de Alcácer, ocurridos en 1993, sucedió algo parecido. Según confirma la sentencia, dos delincuentes habituales, Miguel Ricart y Antonio Anglés, secuestraron a Miriam, Toñi y Desirée, de catorce y quince años, a las que violaron, torturaron, asesinaron y luego enterraron parcialmente y quemaron los restos. El crimen tuvo una gran repercusión en la época y su cobertura mediática se considera el nacimiento de la telebasura en España, en especial por el tratamiento que Antena 3 dio al suceso.

En 1997, en el magazine nocturno *Esta noche cruzamos el Mississipi*, presentado por Pepe Navarro, Fernando García, padre de una de las fallecidas, y el criminólogo Juan Ignacio Blanco acusaron sin pruebas a una variedad de políticos y empresarios valencianos de pertenecer a una trama dedicada a la producción de ese *cine*, que habría sido el principal causante de la muerte de las adolescentes. Estas afirmaciones se repitieron en la televisión valenciana. Como resultado, ambos fueron condenados por calumnias a varios años de prisión y a fuertes indemnizaciones, que superaban los doscientos mil euros.

Hasta la fecha no ha aparecido ni un solo fotograma de la supuesta película *snuff*. Ni de esa ni de ninguna otra, a pesar de que los especialistas en identificación de víctimas de las policías de todo el mundo, coordinados por Interpol, los buscan de forma activa. Eso no quiere decir que no existan intentos más o menos exitosos de colar como reales lo que no son más que filmaciones falsas. Varias de ellas incluso parecían tan reales que han tenido repercusiones legales.

Todavía hoy es habitual ver en las páginas web de fundamentalistas cristianos y activistas islamófobos una muy desagradable imagen que muestra lo que parece una mujer joven semidesnuda, muerta y ensangrentada, tumbada en una cama y con un crucifijo de madera de grandes dimensiones incrustado en la boca hasta la garganta. Dependiendo de la época y el lugar, ese presunto asesinato se atribuye a los Hermanos Musulmanes en Egipto en 2011, a Al Qaeda en Iraq en 2012 o al Estado Islámico en Siria en 2014, acompañado de un texto que, entre soflamas xenófobas, afirma que era una joven cristiana que fue violada y ejecutada por veinte varones *yihadistas*.

Interpol ya tenía conocimiento de esos hechos en una fecha tan anterior como 2006, cuando un ciudadano austriaco entró a la página web del artista quebequés, profesional de los efectos especiales, Remy Couture y encontró un sórdido vídeo llamado *Inner Depravaty* (*Depravación interna*), junto con cerca de mil fotografías. Todas ellas mostraban aparentes torturas y asesinatos de mujeres. Incluían heridas muy llamativas y graves, así como vísceras extraídas de los cuerpos. También estaba el presunto homicida, enmascarado cuando su cabeza era visible, inyectándose heroína o haciendo gestos de desesperación. El examen de los expertos mostró que no había manipulación fotográfica alguna, por lo que el caso se remitió a Canadá para su investigación. No tardó en descubrirse que las actrices que aparecían, que se hacían llamar Amellya, Anne Marie D. y Sophie R., estaban vivitas y coleando y que Couture era un consumado artista del maquillaje cinematográfico. Después de todo, es su forma de vida y ha participado en quince producciones diferentes en ese campo, la mayoría de ellas cortometrajes. No había muerte alguna y no se había pretendido que la hubiera jamás; tan solo era una película *gore* más. Eso no fue suficiente para las autoridades del país norteamericano, que lo acusaron en 2009 de atentar contra la moral debido a que sus obras podían incitar a terceros a llevar a cabo esas atrocidades de manera real. Después de tres años, fue absuelto de todos los cargos e *Inner*

Depravaty puede encontrarse sin problema en los portales de Internet de reproducción de vídeos, donde lo encontraron los creadores del bulo islamófobo y del que extrajeron los fotogramas para usarlos en su campaña.

En 2015 apareció en los foros dedicados a la tortura de la Internet profunda y, de ahí, saltó a los *shock sites* —del estilo de Ogrish— un vídeo que hizo correr ríos de tinta —electrónica— entre los habituales del *gore* más conspiranoicos. Se conoce por el nombre de Greenball, debido a que comienza con un logo consistente en una esfera de la que emana una especie de gas verdoso. A continuación, se puede ver a una mujer joven, rubia, de piel blanca, que viste un top rojo y una falda de color claro, atada a una cama con una cubierta verdosa. El fondo está tapado por lonas negras. Dos varones de gran tamaño, uno de ellos vestido con una camiseta color burdeos, juguetea con un cuchillo sobre la piel de la presunta víctima, y lo hunde en el abdomen y en la vagina. El segundo, de verde, dispara varias veces sobre el cuerpo. Al final, los hombres se apartan, dejando el cuerpo exánime de la chica tendido sobre el lecho, en apariencia muerta. Ha llegado incluso a pasar por real en varios foros de profesionales, a pesar de las numerosas evidencias que muestran que todo es fingido. No hay resistencia apenas por parte de la supuesta asesinada, incluso cuando le abren el vientre con la hoja; una apertura que apenas deja sangre y ninguna víscera. Hay continuos cortes y cambios de plano cada vez que se inflige una de estas heridas y la escena suele quedar oculta por el cuerpo de uno de los supuestos torturadores. Si se observa con detenimiento, se puede apreciar que la hoja del cuchillo se retrae en el mango. Los disparos del arma de fuego resultan falsos a simple vista en un monitor de ordenador, si bien en la pantalla de un teléfono es posible que confundan al espectador.

De manera regular aparecen otros vídeos en el mismo sentido, dado que el morbo es una herramienta poderosa. Por ejemplo *Dafu Love*, en el que se supone que asesinan a bebés con martillos sin ninguna evidencia real, u otro más antiguo en que una mujer, atada a una silla, era torturada hasta la muerte y que también se mostró como un elaborado montaje para páginas sadomasoquistas.

La investigación de las películas *snuff* en Internet se encuentra con muchos obstáculos; no por falta de información, sino por exceso de ella. La cantidad de *ruido* en forma de leyendas urbanas alcanza casi el cien por cien de los casos y, a menudo, de una misma historia se pueden encontrar versiones diferentes, hasta contradictorias. Como mitos que son, siguen sus propias normas. Tienen la vaguedad suficiente para que pueda cuadrar en diferentes personas y situaciones, y no se puede localizar en ningún lugar del mundo un hecho real que encaje con lo narrado. Incluso cuando el suceso ha ocurrido de verdad, como en el caso de No Limits Fun, que veremos a continuación, las leyendas han desplazado a la realidad en la mayor parte de los lugares de la Red, que la deforman cada vez más, de manera muy similar a las historias de tradición oral del pasado.

CUANDO EL MITO SE HACE REALIDAD: NO LIMITS FUN

Hasta la fecha, insistimos, no se ha encontrado ningún vídeo en que se asesine a una persona ante la cámara con propósitos comerciales, pero si alguien es capaz de pensarlo, otra persona puede llevarlo a cabo. Por eso, tal vez en el futuro estemos ante un escenario distinto, en especial, dado el auge de los «vídeos bajo demanda», cada vez más habituales en el mundo del porno, un contacto directo entre el requirente de servicios sexuales y quien lo ofrece, hombre o mujer, bajo precio que se suele abonar a través de sistemas de pago instantáneo pensados justo para ese tipo de transacciones, como Unique Money. El paso siguiente y muy cercano es exigir algo más de los actores. Por ejemplo, que incluyan a uno o varios niños en los *espectáculos*. Eso es casi imposible de conseguir en Occidente, pero en ciertos países del Pacífico existen hasta tramas organizadas para ello, en especial en Filipinas, que parece estar sustituyendo a Tailandia a la cabeza de la explotación sexual infantil. Algunos de estos grupos, ya desarticulados, tenían precio para actos tan aberrantes que pedían sus contratistas como degollar a un animal en el acto sexual con chiquillos o el *juego* con orina o heces. No es impensable que algún cliente pida algo más y encuentre a alguien con voluntad para hacerlo.

En 2013 apareció en los foros más sórdidos de la red TOR un vídeo que venía firmado por un oscuro grupo llamado NLF, acrónimo de No Limits Fun, diversión sin límites en español. Los rumores venían de dos años atrás, pero hasta entonces no se tuvo constancia del mismo. Enseguida cobró una notable popularidad y se hicieron varias versiones, todas basadas en la misma secuencia. Algunas eliminaban el sonido o lo reemplazaban por música. Otras estaban divididas en cada una de las dos escenas del mismo y otras se habían montado como si fueran un tráiler cinematográfico.

Lo que aparecía en él era tan explícito como terrible. En la primera mitad, un bebé que no pasaba de los dieciocho meses, sin ropa, colgado de los pies a medio metro de altura de una cama. Sobre el fondo, posiblemente una tela verde o azul, se han superpuesto imágenes de una *mazmorra*, en tonos verdosos y negros. Una joven, desnuda y enmascarada, tortura a la pequeña, que llora desconsolada por los latigazos y demás vejaciones que le causa. Ambas tienen rasgos asiáticos. Para la segunda mitad, el *croma* del fondo cambia y muestra una suerte de pared gris falsa. La niña mantiene los correajes con los que la han atado al techo, pero ahora está tumbada sobre la cama. La mujer del antifaz vierte cera hirviendo de una vela sobre los genitales de su víctima y luego apoya los suyos propios en la boca, de tal manera que la bebé está a punto de asfixiarse. En varias ocasiones se puede oír a un varón —el que maneja la cámara— dando instrucciones a la mujer en un idioma que cuesta interpretar.

La alarma saltó de forma inmediata entre el Grupo de Expertos en Identificación de Víctimas de Interpol, que no tardaron en encontrar el vídeo, entre otras páginas, en la fenecida Lolita City, dedicada a la pornografía infantil. Algunos pedófilos,

horrorizados por lo que veían, lo denunciaron de forma anónima. La mayor parte de los que abusan de menores racionalizan su conducta entendiendo que es «consentida» y se lleva a cabo «por amor», así que el maltrato les repugna. Hay una pequeña parte de ellos, sin embargo, que no solo se excitan con esas barbaridades, sino que estarían dispuestos a pagar por ellas. Los policías se temían que *Daisy's Destruction*, como se llamaba aquel catálogo de horrores, estuviera dirigido a esa audiencia. Un agente holandés creyó entender alguna palabra en su idioma y de inmediato los Países Bajos lanzaron todo su esfuerzo para tratar de ponerle un nombre a la voz, en especial después de que una copia del vídeo fuera encontrada en poder de un detenido por poseer vídeos de explotación sexual de menores. Inútil. Todavía no lo sabían, pero el idioma que se hablaba era bisayo, originario de varias zonas del Pacífico, sobre todo Filipinas, Indonesia y Malasia, algo que quedaba patente por los rasgos físicos de las dos personas que aparecían en el vídeo. Por ello, la Policía Federal Australiana, uno de los puntales del Grupo y el más cercano a la zona, empezó a tomar cartas en el asunto, en especial en la antigua colonia española, el objetivo más probable. Aun así, el tiempo pasaba y no se conseguía encontrar ni un solo rastro fiable. NLF era muy cuidadoso y no se encontraba ni un solo rastro fuera de TOR que pudiera llevar a su ubicación.

La suerte no es eterna. No lo es para nadie y a veces el exceso de confianza se paga caro. Así pasó en septiembre de 2014. Filipinas es un país que está formado por varias islas. En una de las más grandes, Mindanao, se ubica la ciudad de Cagayán de Oro, cuyo nombre refleja la influencia colonial española. En ella vivían Daisy y Queenie, dos primas que entonces tenían diez y once años. Una mujer, alta y delgada, muy guapa, se acercó a ellas mientras se encontraban, solas y hambrientas, en un centro comercial, no demasiado lejos del mercado tradicional en el que trabajaban sus padres. Entre sonrisas, les ofreció comida, algo que las pequeñas no dudaron en aceptar. Después de llenar el estómago en un restaurante cercano, su benefactora, que dijo llamarse *Ángel*, las invitó a acudir a su casa, donde recibirían más. Las dos pequeñas, entusiasmadas, la siguieron por las callejuelas de la ciudad hasta la parte occidental, donde nuestro conocido *El Americano* las esperaba en una casa con jardín que tenía alquilada. Era, como se ha dicho, un tipo alto y desgarbado, de nariz grande, tez pálida, labios finos y pelo canoso que fumaba mucho y tenía una sonrisa que solo sabían definir como «malvada». Las invitaron a tomar un baño, algo que ambas hicieron encantadas. Esa fue la primera vez que notaron algo extraño, dado que les pareció que el hombre las estaba grabando. Después de eso las condujeron al jardín, protegido por vallas de la curiosidad vecinal, y las obligaron a hacer sendos agujeros, actividad que sería la principal durante los cinco siguientes días. Ambas niñas estaban convencidas de que lo que estaban cavando eran sus tumbas. Después, agotadas, las obligaron a besarse y, acto seguido, a practicarle sexo oral a *El Americano* mientras *Ángel* los grababa. Los hechos habían sido tan horribles que aquella noche, atadas y con una correa de perro en el cuello, ambas consideraron el

suicidio.

Las barbaridades aumentarían en las siguientes jornadas, mientras los hoyos del patio seguían creciendo día tras día. En una ocasión, como Daisy no paraba de llorar mientras el tipo la violaba, Ángel le puso un almohadón en la cara para sofocar sus gritos. Aunque estuvo a punto de asfixiarse, la agresión sexual continuó.

La tercera noche las obligaron a beber alcohol hasta perder el conocimiento. Cuando despertaron al día siguiente, estaban cada una dentro de la cavidad en la que trabajaban, como si fueran a ser enterradas vivas. Los dos adultos les contaron que eso les había pasado por llorar sin parar y querer estar «con su mamá».

El cuarto fue una pura tortura. Por la mañana, tomaron fotografías de cómo cavaban sus futuras tumbas y luego las ataron de pies y manos con cintas de nailon hasta inmovilizarlas por completo.

El último día se les abrió el mundo cuando las dos primas se dieron cuenta de que la puerta estaba abierta y no había nadie vigilando. Ambas salieron corriendo y no pararon hasta llegar al mercado en el que se ganaba la vida su familia, que en todo ese periodo se había desvivido por encontrarlas y se temía lo peor, como había estado tan cerca de pasar. De inmediato contactaron con la policía, que envió efectivos a la casa alquilada. Cuando llegaron, *El Americano* y *Ángel* habían huido a toda prisa, dejando allí evidencias de sus horribles crímenes, incluidas las ominosas excavaciones del corral.

No mucho tiempo después de esos hechos, la policía filipina consiguió atrapar en Cagayán de Oro a la joven, cuyo nombre real, como dijimos, era Carme Ann Álvarez. Ella misma había sido una víctima cuando el violador la secuestró. Entonces tenía trece años. Desde ese momento no había conocido otra vida que la de los abusos sin fin, hasta el punto de racionalizarlos como algo *normal*, dado que era lo que había visto durante la última niñez y la adolescencia. Cuando llegó a los diecisiete, *El Americano* le dijo que ya no servía para seguir saliendo en los vídeos que vendía y su trabajo pasó a ser encontrar otras niñas a las que raptar. No tuvo muchos problemas en contar hasta el último detalle, dado que no entendía del todo la maldad de sus actos con la mayoría de edad recién estrenada y la educación disfuncional que había recibido por parte del monstruo, que, después de todo, era australiano, Peter Gerald Scully, de cincuenta y un años de edad. También habló de una segunda mujer, conocida como *Lovely* —Adorable—, algo mayor que ella y con la misma historia a cuestas. De hecho, era ella la que aparecía azotando al bebé en el infame vídeo.

Al estar presente uno de sus nacionales, la Policía Federal del país del canguro recibió una solicitud del NBI filipino —National Bureau of Investigation, Oficina Nacional de Investigación, equivalente al FBI estadounidense— para colaborar, algo que estaban más que dispuestos a hacer. En primer lugar, descubrieron que el delincuente era conocido allí, un estafador que había defraudado casi tres millones de dólares a veinte inversores y, al ser acusado por la Corte de Melbourne en 2011, tras dos años de investigación, abandonó el país a toda prisa, con destino Manila.

También había sido denunciado por su antigua pareja, una chica malasia muy joven, a la que había vendido como prostituta antes de desaparecer.

Su segunda tarea fue participar en el análisis de dos discos duros que portaba encima *Ángel* y que pertenecían a Scully. En ellos se encontraron pruebas de grabaciones horribles que incluían sexo y tortura con al menos otras seis niñas, desde uno hasta trece años. También se pudo concluir que *Lovely* y Carme Ann eran dos personas diferentes y que los vídeos se estaban vendiendo a través de la empresa No Limits Fun, de la que el buscado era el principal y tal vez único responsable.

El grupo especial del NBI dedicado a este caso, dirigido por Angelito Magno, estaba rastreando, mientras tanto, domicilios de alquiler por todo el país, que, por la forma de pagar y los rasgos de sus autores, pudieran estar ocupados por aquel. En noviembre llegaron a un piso que coincidía con las características buscadas. En su interior había dos adolescentes, encadenadas a la pared por los tobillos. También habían sufrido los abusos del monstruo, que, no obstante, había logrado escapar. De nuevo.

A lo largo de las siguientes semanas se consiguió rescatar a otras cuatro víctimas por todo Mindanao, lo que hacía un total de ocho niñas torturadas y violadas, que pasaron a manos del Departamento de Bienestar Social y Desarrollo del Gobierno. Desde la fuga de las dos primas, Scully ya no podía operar con regularidad. Se veía forzado a estar todo el tiempo huyendo y eso le iba costando más errores a medida que el círculo se estrechaba.

El 19 de febrero de 2015 se localizó a *Lovely* en el aeropuerto internacional Ninoy Aquino de Manila, a punto de coger un vuelo a Cagayán de Oro. Su verdadero nombre era Liezyl Margallo y no le costó nada de tiempo colaborar con las autoridades a cambio de una rebaja en su futura condena, algo que los agentes se vieron forzados a aceptar si querían evitar que se retrasase más la captura del psicópata. Por eso, al día siguiente se pudo montar un dispositivo en el número 2 de la calle Purok, en el distrito de Violeta de la ciudad de Malaybalay, a cien kilómetros al sudoeste de donde Daisy y Queenie cavaron sus propias tumbas. Los agentes esperaron con paciencia hasta que Peter Scully apareció, momento en el que se le echaron encima y pudo ser detenido sin darle ocasión a escapar ni a defenderse. No sería el último.

El siguiente golpe al ánimo en esa trama cruel lo propició *Lovely*. El 25 del mismo mes les condujo a uno de los hogares en los que habían residido, en Villa Corito, en la ciudad de Surigao, con instrucciones precisas de levantar una sección concreta del suelo de la cocina. Debajo de las baldosas había una fina capa de cemento que cedió con relativa facilidad. Ahí estaban los restos mortales, apenas unos huesos, de una niña de doce años que la detenida conocía tan solo como *Barbie*. Según su declaración, la había estrangulado Scully porque las secuelas de las torturas que le habían causado eran demasiado evidentes. Tras hacerlo, hizo un agujero bajo el suelo de la vivienda en el que tuvo que encajarla a la fuerza, dado que era

demasiado pequeño, y lo cubrió de nuevo. El detenido reconoció la muerte aunque la justificó diciendo que «se le había ido la mano», sin más detalles. La siguiente revelación no sorprendió tanto a los policías: el monstruo no actuaba solo. Si bien el asesinato había sido obra exclusiva suya, un alemán había participado en los abusos, tanto físicos como sexuales. Gracias a las aportaciones de ambas mujeres y a los datos recuperados de los dispositivos tecnológicos, se pudo detener al resto de miembros de la red, el germano Christian Rouche —violador de *Barbie*— y los nativos Alexander Lao y Althea Chia. Según los investigadores, las torturas sistemáticas hasta el deceso de los menores parecían una conducta habitual de Scully, que luego vendía a sus clientes a través de NLF. Es posible que los vídeos se grabasen por encargo y que algunos de esos compradores exigiesen el homicidio, como parecía el final al que estaban destinadas las pequeñas Queenie y Daisy antes de su afortunada huida. El hecho cierto es que hasta el momento no han aparecido más restos humanos. El siguiente paso en que están trabajando ahora el NBI y la policía Australiana es localizar a los clientes, diseminados por todo el mundo, que serán detenidos en sus respectivos países por delitos que pueden ser tan graves como los de Scully si se les considera autores intelectuales de las aberraciones, dado que fueron hechas por su petición y para sus fines y ejecutadas bajo precio.

De momento, el sádico y sus secuaces están en prisión preventiva a la espera de un juicio en el que se pide la cadena perpetua. La pena de muerte está en suspenso en Filipinas desde el año 2006, y por ese motivo se librará de la ejecución si es condenado.

Este sórdido caso, uno de los peores que la policía ha tenido que trabajar, muestra la posibilidad de existencia de las películas *snuff*. Hay psicópatas dispuestos a matar por placer, grabarlo y distribuirlo. Los compradores, tras una aséptica pantalla de ordenador y con menos sensación de culpa y riesgo, son legión. Su principal problema está en encontrar víctimas propiciatorias, en especial, niños, a los que casi siempre hay alguien buscando. Por eso no es descartable que en el futuro ocurra algún otro caso, aunque será tan excepcional como el de Peter Scully y sus esbirros y, como este, será perseguido con igual celo y saña por todos los agentes del siempre vigilante Grupo de Expertos en Identificación de Víctimas de Interpol, incluido el Cuerpo Nacional de Policía de España.

ESTAFADORES, ASESINOS Y SUS CLIENTES

La Red no solo nos muestra la muerte, sino que también ofrece formas de buscar a quien la puede causar. Encontrar a personas dispuestas a matar a otros —o, al menos, a darles una paliza— a cambio de dinero es fácil en España, sin necesidad de ordenador. Por ejemplo, a principios de 2015, una vecina de Santa Comba (La Coruña), fue a un poblado chabolista de O Sixto y, preguntando, encontró a quien

matara a su marido por siete mil euros. Sin embargo, los matones se arrepintieron en el último momento y *tan solo* lo dejaron medio muerto de una paliza. Para rematar la chapuza, empezaron a chantajearla y esta los denunció, con lo que se descubrió todo el pastel. Unos años antes, un vecino de Cádiz ofreció dinero a dos marroquíes sin trabajo para una hazaña similar. Sin embargo, los contratados se fueron directos a la policía a contarlo y así se le pudo detener sin más perjuicios para nadie. No tener contactos es arriesgado.

Aquellos que viven con el delito —crimen organizado, traficantes de drogas, etc. — ya saben dónde acudir. Tienen el cauce y la posibilidad de contactarlos. Algunos, incluso, son parte de la propia banda. Caso paradigmático es la banda de Los Miami en Madrid, que empezaron dando palizas de encargo y algún homicidio —fueron acusados de la muerte a tiros del portero de discoteca Francisco Javier Manzanares en Móstoles, en 2001— y después redondearon el negocio con el tráfico de estupefacientes y el control de la *seguridad* de los locales de ocio nocturno de la capital. El ciudadano medio, si no quiere arriesgarse en la calle, como en los casos que hemos visto más arriba, tiene a su disposición Internet, una poderosa herramienta. A principios de la segunda década del siglo XXI no era difícil encontrar anuncios en las zonas abiertas de Internet para encontrar sicarios en España. Solían poner anuncios en páginas gratuitas, incluso alojadas en España, como por ejemplo los de la empresa cántabra Hispavista o la almeriense Creatuforo. Aprovechaban la inmensa cantidad de tráfico de esos sitios para pasar desapercibidos ante los administradores. El 24 de enero de 2012 alguien que se hacía llamar *AlexKudelka2012*, bajo el título «Asesino a sueldo en España e Iberomérica», afirmaba lo siguiente: «Nosotros ofrecemos un servicio discreto, responsable y con total seriedad. A nosotros no nos importan ni sus motivos, ni quién es usted, esto es un trabajo que cuanto menos sepamos el uno del otro mejor que mejor, ¿no cree usted? Por ello si usted necesita una persona que arregle su situación con total seriedad y discreción solo tiene que ponerse en contacto con nosotros. Arreglamos escenarios con el objetivo de que siempre parezca un simple robo, cobramos deudas que para usted han sido imposibles de cobrar, etc.». Ofrecía un correo electrónico como forma de contacto. Publicó hasta siete anuncios similares, incluso comentaba mensajes de otros supuestos asesinos que no habían cumplido lo prometido para ofrecerse a terminarlo. Su forma de hablar parecía indudablemente española. Otros anunciantes que eran incluso más explícitos, ofrecían sus servicios en Colombia, Guatemala o Argentina, si bien algunos se prestaban a viajar a Europa a cambio de la adecuada contraprestación.

Las tarifas de estos asesinos por encargo eran sorprendentes por su escasa cuantía. Solían oscilar entre los mil y los cinco mil euros, a cobrar un veinte por ciento por adelantado y el resto al acabar. En caso de tener que coger un avión, el billete, por supuesto, debía pagarse de antemano. Entre ellos no faltaba quien detallaba los métodos que utilizaría, desde el típico «que parezca un accidente» hasta el

cinematográfico «un pinchazo que no dejará rastro alguno».

La Brigada de Investigación Tecnológica de la Policía comenzó a perseguir todos esos delitos tan pronto tuvo conocimiento de ello. Para eso contactó con las empresas implicadas, que no dudaron en colaborar, puesto que a nadie le gusta que se aprovechen de sus recursos para cometer un delito, menos uno tan grave. De esta manera, en el transcurso de unos meses lograron erradicar la totalidad de anuncios de esas características, que tuvieron que buscar otros lugares en los que hacer publicidad, en especial la red TOR, donde ahora se repiten los mismos patrones con tal similitud que es probable que los autores sean los mismos ya detectados en España. Durante aquella investigación, algunos de los correos de los contactados ya no existían, bien porque los habían dado de baja de forma voluntaria o bien porque habían sido retirados como parte de alguna investigación en algún otro país. Los que contestaron, exigían un pago por adelantado a través de Western Union u otro sistema no rastreable. En cualquier caso, los agentes de la Policía Nacional remitieron los datos de todos los que estaban en el extranjero a través de Interpol y se centraron en los pocos nacionales, como *AlexKudelka2012*, con el que las sorpresas fueron pocas. Una vez identificado, resultó ser un conocido estafador con decenas de antecedentes. Incluso un juzgado había dictado una orden de detención contra él, que se encontraba vigente. Además, su *modus operandi* era diferente a los demás. Quiso quedar en persona, en Madrid, para recibir un pago inicial en efectivo de mil euros, momento en que los agentes detuvieron al esquivo fugitivo. En su declaración, explicó con tranquilidad que era uno más de sus «negocios». Se quedaba el dinero a sabiendas de que quienes lo contrataban no iban a denunciarle por la estafa —no es buena idea acudir a denunciar a quien no ha cumplido tu encargo de asesinar—. Incluso, en ocasiones, les chantajeaba para que siguieran pagando o sería él quien los denunciara.

La experiencia policial indica que la inmensa mayoría de estos anuncios, tanto en la red TOR hoy como en los foros gratuitos de hace un par de años, son de estafadores como el detenido; se puede comprobar al leer los comentarios de los clientes insatisfechos, del estilo «se quedó con mi dinero y nunca cumplió el encargo». Lógico. Es muy extraño que nadie se arriesgue a más de veinte años de prisión por una paga tan exigua. Los delitos contra las personas están muy perseguidos y los que consiguen escapar sin dar cuenta de ellos ante la justicia son poquísimos. Para el caso de los estafadores, la impunidad es enorme, dado que el encaje legal es complicado. Si en realidad nunca han pretendido matar a nadie, solo se les puede acusar del fraude, que tiene una pena mucho más leve y, además, hace falta tener conocimiento de él en primer lugar. El engañado no va a acudir a la policía a contar que no han cumplido su encargo de asesinar a alguien porque se les puede acusar de proposición para cometer asesinato, dado que en su ánimo sí que está causar el mal a una persona concreta. Leer las «ofertas de trabajo» para sicarios da más miedo que los propios matones, porque sitúa a uno ante la dura realidad de que hay cientos de ciudadanos capaces de pagar para que maten a un semejante con todo

el descaro del mundo. Fue significativo el caso de un chaval de trece años que ofrecía tres mil euros para acabar con la vida de su profesora, hasta que la BIT lo identificó y comunicó los hechos, que acabaron con la expulsión del menor y la preocupación de sus padres.

En conclusión, no es fácil contratar a un asesino a sueldo por Internet, a pesar de los muchos anuncios que haya en foros especializados en ello de la red TOR.

EL OSCURO MUNDO DE LO INDECENTE

No podemos acabar un capítulo dedicado a la muerte en Internet sin dar un paseo por alguna de las mentiras más elaboradas que han existido, una vez apartados los falsos casos de *snuff* de los que hemos hablado anteriormente. Uno de los más sonados fue la web *Manbeef.com*, que se podía traducir como «hombre ternera» y que prometía la venta de carne… de seres humanos. En su web, que se lanzó en 2001, se podían ver los *blisters* que ofrecía con costillas, chuletas de pierna, etc. Todo muy limpio y aséptico, tanto que se podían confundir con despiece de cerdo en lugar de hombre. Cada tipo de corte tenía su precio y su peso correspondiente. Sus misteriosos promotores contaban que obtenían la carne de personas «en buen estado de salud» de diferentes lugares del globo, aunque no había forma alguna de adquirirla a través de su página. Tan solo se podían adquirir mercaderías relacionadas, como camisetas o tazas. Llegó a tener medio millón de visitas diarias y, en los foros más retorcidos, los clientes potenciales buscaban alguna manera de conseguir unos trocitos para la barbacoa doméstica. Tal fue el revuelo que el Departamento de Alimentos y Medicina de los Estados Unidos, el equivalente a nuestro Ministerio de Sanidad, lanzó una investigación en profundidad que determinó que, de hecho, no se vendía carne humana por ningún sitio. Abrumados por el sorpresivo éxito, los *webmasters* salieron a la luz. Eran dos jóvenes, Chris Ellerby y Joseph Mallett, cuyo propósito tan solo había sido *provocar a los internautas más sensibles*, aunque en realidad lo que consiguieron fue poner en evidencia a un montón de tipos deseosos de convertirse en caníbales sin riesgo alguno.

5

LOS NEGOCIOS ILEGALES

Australia es un país complicado para que un pequeño camello se gane la vida. Es una isla que está lejos de casi cualquier sitio. Las drogas han de venir de otros continentes, por lo que son caras y obtenerlas, arriesgado. El gobierno no duda incluso en utilizar la aviación de guerra para hundir los barcos que traen la preciosa mercancía. El negocio de Paul Leslie Howard, de treinta y dos años, dedicado a la venta online acababa de quebrar. Su mujer también estaba en paro y no veía forma alguna de salir adelante de forma legal, menos aún con la crisis rampante que ahogaba la economía en aquel 2011. Decidió aprovechar sus conocimientos en Internet y en el mercadeo electrónico para mirar al futuro con entusiasmo. Conocía la red TOR y no tardó en encontrar un auténtico supermercado negro conocido como Silk Road (la Ruta de la Seda, en inglés, como homenaje a los caminos comerciales que unieron Europa con el Lejano Oriente desde tiempos de los romanos). Entre sicarios, armas y otros objetos peligrosos, lo que más le llamó la atención fueron los estupefacientes. Además de ser los más abundantes y lo que más éxito tenía, su precio era barato para los estándares europeos, mucho más para la tierra de los canguros. Ofrecían envíos a cualquier parte del globo con cargos razonables y las opiniones de los clientes eran más que satisfactorias. Hizo sus primeros pedidos de comprobación, que llegaron vía postal a su domicilio en sobres discretos que simulaban tener correspondencia. La pureza era extraordinaria. Así, se lanzó a un lucrativo negocio que le proporcionó miles de dólares en poco tiempo. Los envíos le llegaban en diversos envoltorios, desde cajas para DVD hasta en tarjetas de felicitación e incluso dentro de un termómetro. Llegaban de Holanda y Alemania. Cada vez fue aumentando su oferta, que incluía sobre todo éxtasis y cocaína, aunque también LSD. Tenía dos teléfonos móviles con los que canalizaba los pedidos que iba recibiendo, casi siempre a través de mensajes de texto. El negocio iba viento en popa. Hasta empezó a revenderlas en el mismo portal ilegal donde las adquiría. Sus compradores recibían en sus pantallas escritos como «tengo cinco mil dólares en cocaína, si te interesa» o «promociona más el LSD; la semana pasada vendí 200 dosis». Todo sin salir de su casa y casi por los mismos medios que usaba en su quebrada empresa legítima. Demasiado llamativo para la Policía Federal Australiana, que empezó a seguirle la pista y detectó hasta once envíos diferentes, sin contar todos los anteriores. El 12 de julio de 2012 registraron su domicilio y se llevaron catorce gramos y medio de cocaína y casi cincuenta de MDMA (el principio activo del éxtasis). Poca cantidad, pero comprensible, dado que lo remitía al poco de recibirlo. Funcionaba bajo demanda, con un bajo o inexistente almacenaje. También tenía balanzas de precisión, bolsitas autosellables, dos mil trescientos dólares

australianos, treinta y dos tásers disfrazados de teléfonos móviles… y más de diez mil textos en su teléfono incriminándolo. Abrumado por las evidencias en su contra, se declaró culpable ante un tribunal en febrero de 2013. El juez Damien Murphy, encargado del caso, declaró que las actividades de Howard eran lo más parecido a una venta desde un garaje —haciendo referencia a la tradicional actividad anglosajona de vender los trastos viejos en un tenderete montado en la cochera de una casa unifamiliar—, pero a través de Internet. La sentencia fue benévola, tres años y medio de cárcel, teniendo en cuenta que se arriesgaba a pasar entre rejas hasta veinticinco.

Al sitio web de TOR no le quedaba tampoco mucha más vida…

EL MERCADO NEGRO EN INTERNET ABIERTO

La evolución de la sociedad ha ido prohibiendo el comercio de ciertos bienes. En algunos casos, de aplicación casi universal —como artefactos de destrucción masiva —. Otros, depende de la zona del mundo. Mientras la vieja Europa, baqueteada por siglos de guerras, tiene como supremo bien jurídico proteger la vida y, por tanto, las armas de fuego —de «defensa personal»— están muy restringidas, en Estados Unidos y algunos países africanos, su tenencia no solo es lícita, sino hasta un uso social. Las drogas son otro lucrativo negocio cuya ilegitimidad empieza a estar en duda. Su uso recreativo está perseguido en la inmensa mayoría del mundo porque su popularización fue posterior al desarrollo de la medicina. De otro modo, el tabaco y el alcohol también formarían parte de las sustancias ilegales. Alguna voces reputadas piden cada vez con más fuerza su regulación, algo que se está considerando para algunas plantas cuyos efectos se consideran «blandos», como el *cannabis sativa*, de hecho autorizado en Holanda, y para consumo personal —o sea, fuera del comercio — en muchos países, incluida España. El hecho es que la ilegalización de algo que tiene un mercado gigantesco ha propiciado la aparición de mafias y crimen organizado a una escala tan alta que están en condiciones de tomar el poder *de facto* en países en los que representan una de las mayores aportaciones al Producto Interior Bruto, como ocurrió con la cocaína en la Colombia de los noventa con Pablo Escobar y el cártel de Medellín, o en la actualidad sucede con las organizaciones mexicanas. Al otro extremo del mundo, buena parte de la financiación de las bandas afganas y de los talibanes provenía de la heroína.

Después, están todos los productos y servicios que la lógica y el derecho natural —además del de los estados— dictan que están mal, sobre todo ataques a las personas y a la propiedad, empezando por los sicarios de los que hemos hablado en el capítulo anterior. También números de tarjetas robadas, accesos a diferentes páginas de pago, acciones de *hackers* para perjudicar a la competencia o adquirir documentación falsa con la que luego cometer otros delitos, por poner tan solo

algunos ejemplos. Casi cualquier cosa se puede comprar y vender si se sabe dónde buscar.

Para que un negocio de esta clase funcione solo hacen falta dos requisitos: que el cliente pueda encontrar al proveedor y que el dinero pueda cambiar de manos sin llamar la atención. Para lo primero, Internet es el medio perfecto. Se puede llegar a una gran cantidad de personas sin necesidad de exponer el físico, a menudo desde la comodidad del hogar. Si se dominan los medios de anonimizar la conexión que hemos visto en el primer capítulo, se obtiene, además, una razonable seguridad personal. El problema viene a la hora de cobrar, porque la única forma de que el dinero no sea rastreable es una entrega en mano de billetes, pero eso conduce de nuevo al riesgo de un encuentro personal con quien puede ser un policía o, peor aún, un malintencionado agresivo. Los pagos *online* dejan una huella notoria y las plataformas dedicadas, como PayPal, suelen incorporar un departamento antifraude para detectar irregularidades. La solución tradicional pasaba por realizar envíos de remesas a través de empresas como Money Gram o Western Union, algo que no está exento de riesgos, a menos que el delito lo cometa una organización que pueda permitirse pagar a testaferros —como mendigos o yonquis— para que retiren los envíos o bien aprovecharse de una legislación con laxitud suficiente para hacer esos ardides innecesarios. En la Unión Europea, España incluida, es difícil conseguirlo. Hace falta algún tipo de sistema que escape del control gubernamental y que permita transacciones seguras. Tiene que gozar de una aceptación suficiente, que sea fácil de obtener y que sea legal. Eso existe desde 2009 con la creación de Bitcoin, una moneda virtual descentralizada que tiene una tasa de intercambio con el euro, el dólar y las principales divisas nacionales. Y sin control. Es ideal para cobrar por algún delito.

El cliente capaz de manejarse en la Internet profunda con soltura suele convertirse con rapidez en desconfiado. Si no hay forma de saber quién está detrás, ¿cómo se puede garantizar que no me vayan a estafar? Más teniendo en cuenta que los pagos con Bitcoin no son rastreables y que tampoco va a poder denunciar si no le llegan las drogas o si su víctima no es asesinada. Se puede obtener una cierta seguridad de dos maneras. Por un lado, que el vendedor sea recomendado por un número alto de clientes. Dos o tres votos positivos pueden ser engañosos —quizá el propio comerciante con varias identidades supuestas— y, al contrario, un porcentaje de negativos superior al uno por ciento son una sentencia. El segundo sistema es todavía mejor, pero requiere un intermediario de plena confianza, alguien que mantenga retenido el dinero hasta que la entrega se realice. Ambos sistemas están vigentes en las más importantes páginas legales de venta entre particulares de Internet —como eBay, por ejemplo—. ¿Podría alguien implementarlos también en las zonas oscuras de la Red?

Antes de la popularización de TOR, el mercado negro de Internet ya funcionaba, hasta con menos recelos. Aunque los sistemas ya existieran, de poco sirve utilizarlos

si no hay un número suficiente de personas para crear una masa crítica de clientes potenciales. La primera década del siglo fue más ingenua, también entre los criminales. Entre 2004 y 2005, la Policía Nacional llevó a cabo en España la Operación Ruber50. Empezó al detectar a un pederasta muy activo que estaba, a toda costa, intentando quedar con un menor de edad para acostarse con él. Los familiares denunciaron los hechos, que concluyeron con su detención por la Brigada de Investigación Tecnológica. Por el estudio de la gran cantidad de datos incautados se descubrió una trama en que varios individuos abusaban de niños o les pagaban por acostarse con ellos. Además, se anunciaban en diversas páginas de Internet para vender cedés con pornografía infantil. No la que ellos producían, que guardaban con celo, sino lo que se descargaban de Internet y que luego remitían por correo a cambio de diferentes cantidades de dinero, que solían rondar los cincuenta euros. Los agentes encontraron recibos de los envíos de Correos a dieciséis personas repartidas por toda España, que fueron detenidas. A pesar de no utilizar sistemas para protegerse, su actividad había pasado desapercibida y solo el arresto de uno de ellos consiguió desvelarla.

En 2010, en una operación en la que participó la Policía Nacional se detectó una serie de mensajes en una popular página de anuncios de la Red, en la que un individuo que se hacía llamar *Pepecruz* ofertaba titulaciones de estudios por encargo. Iban desde diplomas de la ESO o de Bachiller a grados universitarios, pasando por certificados de nivel de lengua catalana. Por ello solicitaba cifras que oscilaban entre los trescientos y los mil setecientos euros. Los pagos por los encargos debían hacerse a su cuenta bancaria, lo cual tampoco era muy sofisticado. Para dificultar en cierta medida la acción policial, cambiaba de correo electrónico cada poco tiempo y las anotaciones bancarias figuraban con conceptos falsos, como regalos de boda o entrega de mobiliario. Fue detenido en Mataró (Barcelona), donde se le intervino material para realizar las impresiones de los títulos con calidad suficiente y cuatro mil euros en efectivo. Se le pudieron demostrar unos beneficios de unos veintidós mil. La investigación continuó y se localizaron dieciséis compradores, que fueron imputados por delitos relacionados con la falsificación de documentos —tan culpable es quien la hace como quien encarga hacerla— y, más importante aún, tres detenidos que estaban, de hecho, usando la titulación comprada para trabajar, haciéndose pasar por quienes no eran. Entre ellos destacaba uno que había encontrado empleo en una importante entidad bancaria española gracias a un diploma de Dirección y Administración de Empresas cuya titulación no poseía. Basta con buscar en Internet un poquito para obtener lo que se desea, para suplir con dinero lo que no se ha sabido lograr con esfuerzo.

Un campo en que los tramposos buscan ayuda ilegal con prontitud es el de los gimnasios. Personas que desean conseguir pronto volumen muscular tienen la tentación de recurrir a la farmacia. Anabolizantes, esteroides, hormona del crecimiento… hay un gran abanico de sustancias para ello, que se deben tomar en un

orden determinado. Estos inyectables y pastillas son legales. Se fabrican en diversos laboratorios de todo el mundo para tratar determinadas dolencias entre las que no se incluye, desde luego, lucir bíceps frente al espejo. Su uso, más aún en las altas dosis que requieren —entre diez y sesenta veces lo prescrito de manera legal— tiene graves efectos secundarios, como la impotencia crónica y accidentes vasculares. Para contrarrestarlos, toman otros fármacos. La secuencia determinada de consumo, que dura varias semanas, es lo que se conoce como *ciclo* en su argot y, del mismo modo, *ciclado* es quien obtiene de ello su desarrollo físico. Por ese motivo, este comercio, si bien legal, está muy restringido y es necesaria receta médica. Algunos consumidores consiguen falsificarlas o tienen algún galeno de su confianza al que recurrir. Son los menos. La mayoría de tramposos recurre a Internet. Es muy fácil encontrar foros y blogs en los que se indican las proporciones, los plazos y el principio activo a introducir en el organismo, con títulos tan obvios como «tu primer ciclo de esteroides». Ya solo queda bucear en las páginas de anuncios para saber cómo comprar; donde hay clientes, habrá proveedores. A menudo son también *ciclados* que buscan subvencionarse sus propias medicinas con lo que otros les paguen. Para ello, las adquieren en grandes cantidades en países que no tienen el estricto control que hay en España, y luego montan su propia red de distribución. Debido a su forma de adquisición, sin garantía alguna, en ocasiones el producto está adulterado o caducado y no es raro que solo contenga agua u otro excipiente inocuo. Los riesgos de su uso son muchos estando en buenas condiciones. Pueden ser incluso mortales, lo que no disuade a la mayoría de los dispuestos a jugar con su cuerpo.

La Unidad de Investigación Tecnológica mantiene una supervisión continua, con la colaboración de los administradores de las principales páginas de anuncios en Internet, y gracias a ello, entre 2007 y 2012, detuvieron a veintidós traficantes e incautaron veintidós mil dosis y treinta y cinco mil euros en efectivo. Además, se cerraron ciento cincuenta enlaces de venta, solo en España. Por contra, en los siguientes tres años, los porcentajes bajaron hasta solo nueve detenidos, con cincuenta mil dosis y veinticuatro mil euros. Las páginas cerradas disminuyeron hasta ochenta y siete. Los números no mienten. Los delincuentes se van desplazando hacia la Internet oculta, en especial la red TOR, para evitar en la medida de lo posible la acción policial, dado que hoy ya hay una cantidad de usuarios suficiente para tener la masa crítica que antes citábamos.

En fechas tan recientes como 2014 cayó una red que vendía droga a través de Internet, ignorantes del compromiso que los administradores de las webs españolas tenían con su erradicación. En foros públicos —como los de *Ya.com*—, blogs y redes sociales ponían anuncios tan explícitos como «vendo cocaína 95 de pureza» o «venta cocaína en Madrid entrega en mano», que afirmaban traer «de Bolivia y países aledaños». Para contactar con ellos siempre proporcionaban una dirección electrónica de Gmail —por tanto ubicada en la Internet abierta—. Un ciudadano encontró uno de esos tan poco discretos avisos y dio parte a la Policía Nacional a través del correo

para colaboraciones anónimas *antidroga@policia.es*. Al principio, parecía que los responsables podían ser como el australiano con el que hemos empezado el capítulo, que comprasen el material a un minorista que se anunciase dentro de alguna página estilo Silk Road —por entonces ya desmantelada, pero que no ha tardado en tener sucesores— y luego lo revendiese. Novedoso, pero nada extraordinario por su volumen. Sin embargo, las investigaciones apuntaron a un grupo organizado con más recursos de los esperados. Tenían entre los suyos a un empleado de una compañía aérea y a otro de una de mensajería. Entre los dos conseguían introducir en España la sustancia camuflada como paquete postal. Otras remesas llegaban vía *muleros* —gente que la introduce en su cuerpo y luego la expulsa en destino o la lleva entre sus pertenencias—. Uno de estos cayó en Guayaquil (Ecuador) con nada menos que nueve kilos. En el aeropuerto de Madrid se interceptaron tres envíos que sumaban otros cinco, destinados a otros tantos miembros de la red que vivían en Madrid y Santander. Más tarde se logró atrapar a dos camellos que viajaban con un par de kilos desde Torrevieja (Alicante) hasta la localidad madrileña de Alcobendas, en la que se halló un centro de adulteración. Allí mezclaban la cocaína con otras sustancias más baratas —lo que se conoce como *cortarla* en el argot—, de manera que duplicaban o triplicaban la cantidad a costa de una disminución equivalente de su pureza. Al venderla en Internet por el precio minorista del producto original, multiplicaban sus ganancias. Una vez ubicados todos los miembros de la trama, se realizaron las detenciones y los registros en sus domicilios en los que se encontraron dieciséis kilos y medio adicionales, cuatro vehículos, dos armas blancas y su medio de trabajo, cuarenta teléfonos móviles —los delincuentes suelen tener multitud de líneas al mismo tiempo para contactar con sus clientes y dificultar que se los *pinche* la policía— y tres ordenadores portátiles con los que colgaban los anuncios y respondían a los correos electrónicos.

Desde hace años, y cada vez con más intensidad, la policía mantiene una vigilancia continua sobre los posibles artículos de venta ilegal que se lleva a cabo desde proveedores españoles. Además, colabora con las organizaciones internacionales para la localización y arresto de los que son detectados en el extranjero. La red TOR, Freenet, I2P son un nuevo desafío, pero en ningún caso representan una impunidad absoluta.

EL CASO SILK ROAD

TOR es, entre otras cosas, un gran mercado de ilegalidades sin control alguno. Amparados en la falsa sensación de impunidad, desde pequeños delincuentes a grandes traficantes ofrecen sus productos y servicios a cambio de monedas virtuales, sobre todo la famosa Bitcoin. ¿Quieres desactivar la página web de un negocio rival? Lo puedes conseguir por poco más de diez euros por hora. ¿Quieres convertirte en un

spammer y enviar publicidad de tu empresa a un millón de correos electrónicos de todo el mundo? Hecho, si pagas entre trescientos y ochocientos euros. ¿Quieres datos de una tarjeta de crédito o de una cuenta de PayPal para comprar en nombre de un tercero, y con sus fondos, no con los tuyos? Lo tienes desde un euro para datos antiguos —de más de un día desde que fueron robados— hasta trescientos por una Visa Platino recién sustraída y sin límite de gasto. Si lo tuyo es la documentación falsa, puedes tener un permiso de conducción para el país de tu elección por cincuenta euros para las falsificaciones más burdas, hasta dos mil quinientos para un carné indistinguible —más o menos— de uno real. ¿Un arma de fuego? Puedes adquirir las más baratas por poco más de cien dólares, aunque lo complicado, por lo menos en España, es hacértela llegar a través de la aduana.

Y, sobre todo, en TOR se vende droga, de todos los tipos y de gran calidad, sobre todo al consumidor final o pequeño traficante. Por ejemplo, en Alphabay, uno de los mercados punteros de productos ilegales en 2015, donde hay vendedores que envían a todo el mundo, el gramo de cocaína ronda los setenta euros, algo más del precio medio en España, que está en torno a sesenta, pero mucho más barato que en Estados Unidos, donde pasa de los ciento ochenta, o de Australia, donde cuesta más de doscientos. Un coste similar al de la heroína, que se dispara en el país austral hasta los trescientos setenta. El cannabis se obtiene a unos tres euros el gramo, parecido al precio europeo y de nuevo lejos de los catorce de Norteamérica o diecisiete de Oceanía. Aquí, por tanto, hay poca diferencia económica al adquirir las sustancias al camello habitual del barrio o hacerlo en uno de estos con nombres tan poco discretos como «Drogas desde Alemania»… salvo por el control de calidad y la devolución del dinero en caso de insatisfacción. Estos mercados solo hacen de intermediario. De una manera muy parecida al portal de subastas eBay, los vendedores, que son particulares no asociados con la web donde se alojan más allá de pagar una comisión por venta efectuada, reciben un voto por cada intercambio, que puede ser positivo, negativo o neutral. Se valoran factores como la calidad del producto, la discreción o rapidez en el envío. Un *comerciante* que está empezando lo tendrá difícil hasta que obtenga las suficientes aprobaciones de sus compradores. Uno que haya sido rechazado por la mayoría tendrá muy difícil hacerse un hueco en el mercado. La consecuencia inmediata de esto es que la calidad de los estupefacientes adquiridos *online* está muy por encima de sus equivalentes físicos, como ha podido comprobar el laboratorio español Energy Control, que se dedica a analizar la pureza de todo tipo de sustancias ilegales que son remitidas por particulares de todo el país. Si vendieran productos adulterados, caerían con rapidez en su prestigio y, por tanto, en sus ventas. Muchos de estos pequeños traficantes, además, ofrecen un servicio de reembolso con condiciones acordadas de antemano. Pueden especificar que, si no quedas satisfecho, te devuelven el cuarenta por ciento de lo pagado o hasta el total si eres su cliente habitual, con al menos diez transacciones. Ante estas ventajas, en nuestro país la compra por Internet ofrece grandes ventajas; a un adicto estadounidense o australiano

le resulta una verdadera bicoca.

Alphabay no fue el primero ni el más importante de estos mercados negros virtuales. Dejando a un lado The Farmer's Market —*el mercado del granjero*—, se puede decir —aunque no sea del todo cierto— que todo empezó con Silk Road, «La Ruta de la Seda». Hay que remontarse hasta 2011 para encontrar a un individuo que se hacía llamar el *Temido Pirata Roberts* (*Dread Pirate Roberts*), en claro homenaje al protagonista de la novela de William Goldman y posterior película de culto *La princesa prometida* (*The Princess Bride*, Rob Reiner, 1987). Como él, escondía su verdadera identidad tras una máscara —en este caso, el enrutamiento TOR en vez de un trapo negro sobre su rostro— y, durante un tiempo se temió, de forma infundada que, como su sosias, no fuese una persona sino una pluralidad; es decir, que se llamaba *Dread Pirate Roberts* a quien estuviera administrando esos negocios ilegales en un determinado momento. El mismo *Pirata* jugó con eso al afirmar a la revista *Forbes* en una entrevista en que no se desvelaba su identidad, que él era tan solo el que había *heredado* la empresa del anterior dueño. Sin embargo, al contrario que el de ficción, el real tenía unos propósitos mucho más oscuros que encontrar «el amor verdadero». El hombre detrás del apodo se llamaba Ross William Ulbricht, un tejano de Austin, nacido el 27 de marzo de 1984, de pelo castaño alborotado y ojos verde oscuro. Estudió en la Universidad de Dallas, en la que se graduó en Física en 2006. Poco después se sintió atraído por teorías libertarias y contra todo tipo de regulación estatal. Su ídolo era el político y filósofo republicano —y antiguo miembro del Partido Libertario, que lo propuso como candidato a presidente de los Estados Unidos en 1988— Ron Paul, cuyas ideas, según él mismo, se resumen en que «la función correcta del gobierno es proporcionar la defensa nacional, un sistema legal para disputas civiles, una justicia penal para casos de agresión y fraude y poco más».

Ulbricht inició una carrera de especulador a corto plazo —mediante la técnica conocida como *day trading*, que consiste en comprar bienes, sobre todo productos financieros, y venderlos el mismo día, aprovechando las fluctuaciones del mercado— que no tardó en fracasar. Después lo intentó, con la misma suerte, con empresas de videojuegos y una librería de reventa en su ciudad natal, llamada Good Wagon Books, que se hundió —literalmente: colapsó bajo el peso de los cincuenta mil volúmenes que guardaban en ella—. En 2010 conoció la moneda virtual Bitcoin. No tardó en descubrir su potencial, sobre todo su falta de control gubernamental, que permitía pagos casi indetectables. Alrededor de ella crearía el proyecto de su vida, siguiendo sus propias directrices morales y políticas, la página web Silk Road. Según su propia definición, que plasmó en su diario personal, «la idea era crear un sitio web donde la gente pudiera comprar cualquier cosa de forma anónima, sin rastro alguno que pudiera detectar quiénes eran». La alojó en un servicio oculto de TOR al que solo se podía acceder a través de este sistema. Eso significaba, como ya hemos visto, que era en extremo difícil saber dónde se encontraba alojada o quién la manejaba. Después de un periodo de desarrollo y programación de seis meses, el sitio vio la luz

en febrero de 2011. Estaba pensado como un «mercado anónimo total» en el que se podía vender todo tipo de productos sin control gubernamental alguno, tanto legales como ilegales. Como es lógico, los segundos eran casi la totalidad. De hecho, solo los diferentes tipos de drogas llegaron a ser el setenta por ciento del total de lo ofrecido. Para comerciar con sillas de jardín hay sitios menos complicados donde hacerlo. El uso de Bitcoins la diferenciaba de sus antecesoras, como la mencionada The Farmer’s Market, que utilizaba servicios como Western Union o PayPal, más fáciles de investigar. No obstante tenía un cierto código moral, ya que prohibía bienes robados, pornografía infantil y titulación falsa. Por otro lado, permitía y hasta apoyaba que incluso niños pudieran acceder y comprar.

La web se identificaba con un dromedario verde sobre el cual se encontraba sentado un beduino, referencia a los comerciantes que cruzaban desde China hasta Europa en la Edad Media, siguiendo la Ruta de la Seda original, de la que había tomado el nombre. A la izquierda, debajo del logotipo, estaba el listado de bienes y productos, que comenzaba con un listado de drogas, clasificado por su tipo: cannabis, disociativos, éxtasis, opiáceos, psicodélicos, estimulantes… Incluso se vendían precursores, para que el cliente pudiera sintetizar en su propio domicilio. A continuación, el resto de servicios y materiales, desde tarjetas de crédito a supuestos asesinos por encargo. También fuegos artificiales, artículos eróticos y un largo etcétera casi vacío en muchos casos. Por ejemplo, en la categoría de pirotecnia apenas se ofrecían un par de elementos a la venta.

En la zona central de la pantalla se podía acceder al detalle de los elementos a la venta, unos doce a la vez, cada uno de los cuales iba identificado por una fotografía con su rótulo (como «4 gramos de cocaína, escamas de cristal puras») seguida del precio, en Bitcoins, un problema para el usuario medio. Al carecer de control alguno, su precio puede fluctuar hasta un sesenta por ciento de un día a otro, por lo que había que tener una tabla abierta con las equivalencias del momento. Dependiendo del momento y de la agilidad del vendedor, la misma cantidad podía costar trescientos o ciento veinte euros al cambio. Haciendo clic en cada imagen se accedía a su página de venta, donde se mostraban detalles de la sustancia y de la transacción, como a qué regiones del mundo se enviaba, si existían gastos de transporte, en qué condiciones (por ejemplo en sobres que simulaban contener postales de viaje). Otro detalle más importante aún era el sistema de pago, que podía ser directo, entre cliente y vendedor, o indirecto, donde el dinero quedaba retenido por un intermediario, que era la propia web, hasta que se recibía el material solicitado, como control para evitar fraudes. Por último, se podía acceder a la página del mercader y observar el número de transacciones y la puntuación —positiva, negativa o neutra— que había recibido de sus otros clientes. También los compradores eran evaluados de la misma manera y alguien que no tuviera una buena reputación virtual no conseguiría que nadie estuviese dispuesto a venderle.

A la derecha de la pantalla principal había un apartado para «noticias», como la

apertura del portal hermano The Armory, La Armería, que quebró en poco tiempo por falta de ventas. Para completar el interfaz, en la parte superior se podía acceder a un servicio de mensajería privado con el que contactar con el administrador o entre usuarios.

¿Y qué sacaba el *Temido Pirata Roberts* de todo esto? ¿Dónde está el negocio después de invertir bastante en poner en marcha todo el tinglado? Por cada transacción efectuada a través de Silk Road se embolsaba entre el seis y el quince por ciento de su valor. Es decir, dados los costos de desarrollo y operación, para ser rentable necesitaba una cantidad alta de ventas o un precio muy alto de las mismas. Lo segundo era ocasional, dependiendo, sobre todo, del servicio a prestar. Lo primero lo consiguió cuando Gawker, uno de los blogs más seguidos del mundo —veintitrés millones de visitas mensuales—, de referencia para el neoyorquino medio en especial, le dedicó un artículo cuatro meses después de que el mercado hubiese empezado a funcionar.

Para el cliente, hacerse una cuenta en Silk Road era gratuito, cuestión de registrarse y a comprar. El vendedor tenía que hacer un cierto desembolso económico. Al principio, había un número limitado de nuevas cuentas, que se ofertaban en pública subasta y ganaba el mejor postor. Más tarde, se abrió la posibilidad de registro abonando una cantidad fija que podía llegar, según la fluctuación de la Bitcoin, a los cuatrocientos euros.

Uno de esos vendedores, especializado en marihuana, era el canadiense Roger Thomas Clark, que se hacía llamar *Variety Jones*, conocido además por su oposición a la guerra contra las drogas. No tardó en contactar con Roberts, con el que forjó una buena amistad además de un lucrativo tándem al que también se sumaría un misterioso personaje, cuya identidad a día de hoy se ignora, que se hacía llamar *Smedley* y llegó atraído por el artículo de Gawker y se dedicó a implementar mejoras técnicas como programador, incluido el proyecto de correo electrónico SilkMail, que dejó sin finalizar.

Variety Jones se convirtió en el consejero de Ulbricht, programador, auditor de seguridad —esto es, si el sitio era vulnerable a ataques de *hackers* o de la policía— e, incluso, relaciones públicas. Juntos hicieron mucho dinero. Tanto que, en el momento de ser desmantelado, el 2 de octubre de 2013, se calcula que el beneficio total obtenido por el sitio en conjunto era de mil doscientos millones de dólares, de los cuales, los administradores habían ganado casi ochenta en concepto de comisiones. Eso en poco más de dos años y medio.

Como es natural, Gawker también lo leen las fuerzas de seguridad. Además, eran ya multitud los paquetes con droga que habían interceptado antes de que llegasen a sus compradores. Se creó un equipo conjunto en Baltimore en el que participó la DEA (la agencia antidroga), el Servicio Secreto, Hacienda, Seguridad Interior e Inspección Postal. Al mismo tiempo, los expertos en cibercrimen del FBI estaban trabajando a todo ritmo en Nueva York. Mientras los primeros aplicaban los

procedimientos tradicionales de las investigaciones de estupefacientes, siguiendo el hilo desde el último enlace hasta la cabeza, los segundos tomaban un camino diferente, el de su especialidad. Sabían que la cadena de traficantes no es como la red funciona, y que, además, el *Temido Pirata Roberts* no producía ni importaba droga, sino que tan solo proporcionaba la manera de que los que la tenían la hicieran llegar a sus consumidores finales.

Uno de los primeros éxitos de la gente de Baltimore les llevo a Utah, el estado de los mormones, en enero de 2013. Habían detectado un envío de un kilo de cocaína a nombre de un tipo de cuarenta y siete años llamado Curtis Clark Green y fueron a buscarle a casa. La sorpresa para todos fue que habían dado con un tipo llamado *CronicPain*, (Dolor Crónico), que era uno de los administradores de Silk Road, contratado por el propio *Pirata Roberts* para que se encargase de la atención al cliente. En efecto, la complejidad del sitio estaba siendo tan elevada que, además de programadores y consejeros de seguridad, necesitaba un abanico de otras especialidades.

El envío de cocaína no había sido accidental. La persona para la que Green pensaba que iba a actuar de intermediario era un agente de la DEA. Lo que no esperaban era que el tipo en cuestión tuviera una posición tan relevante en el *ranking*… aunque sirvió de poco, porque el detenido no había visto jamás a su jefe ni tenía más pistas de él que los investigadores. El salario lo recibía en Bitcoins y las conversaciones eran a través del chat encriptado *Torchat*, por lo que no había manera de rastrearlo. Estaban tan lejos como al principio, aunque en breve iban a aprender algo nuevo, que el tipo libertario, con principios y ganas de ayudar a los demás no dudó en ordenar el asesinato de su antiguo empleado.

Otro de sus consejeros de confianza era *Nob*, un dominicano tuerto que gestionaba un gran negocio de importación de droga a los Estados Unidos y que había intentado comprar Silk Road —aunque desistió cuando el dueño le pidió mil millones de dólares—. *El Pirata* recurrió a él, al que tenía por un hombre de recursos. *Variety Jones* le había convencido de que Green tenía que morir, dado que tenían miedo de lo que pudiera contar a los agentes que le habían detenido y sospechaban que tenía información que podría comprometer toda la empresa. Además, afirmaban que había robado trescientos cincuenta mil dólares en Bitcoins. Pagó ochenta mil para ver cumplidos sus deseos. Lo que Ulbricht no sabía era que *Nob* tampoco era quien decía ser, ni dominicano, ni tuerto, ni regentaba un imperio criminal. Era Carl Mark Force IV, otro agente de la DEA del grupo de Baltimore y quien tenía en custodia a *CronicPain*. Con la anuencia del arrestado, que de hecho ya les había contado que temía por su vida, simularon un espectacular ahogo en una bañera —demasiado *entusiasta* para su protagonista— que fotografiaron como prueba de que el encargo se había cumplido. Los *autores* fueron un inspector postal y un miembro del Servicio Secreto, disfrazados a conveniencia. De esta manera, *Nob* se ganó la confianza del Ulbricht y comenzó su lento camino para conseguir verlo algún día, momento que

aprovecharía para detenerlo, por fin. Mientras tanto, seguía ganando millones y pensando en nuevos asesinatos.

En marzo de 2013 la tomó con un usuario que se hacía llamar *FriendlyChemist*. Había sido estafado por un supuesto vendedor de Silk Road llamado *LucyDrop*, que se había quedado con su dinero pero no le había enviado las drogas, de modo que había contraído una deuda de medio millón de dólares por la que le iban a matar. Por ello, empezó a chantajear a Ulbricht, que, ni corto ni perezoso, tomó la iniciativa. Pagó ciento ochenta mil dólares a un tal *Redandwhite*, que afirmaba ser miembro de los Ángeles del Infierno, por verlo muerto. A la lista se sumaron después un estafador conocido como *Tony76* y sus tres compañeros de piso, a estos últimos tan solo por la sospecha de que podían conocer las actividades de su colega. Con los sucesivos regateos, acabó pagando más de un millón de dólares para acabar con los cinco. Le había cogido el gusto a eliminar a aquellos que le pudieran causar un problema, algo que le resultaba fácil, dado lo aséptico de la situación, desde la comodidad de su hogar, sin ver la sangre ni el sufrimiento ajeno. Sin embargo, nunca apareció ningún cuerpo. Tampoco su dinero. Como escribió en su propio diario en algún momento entre junio y noviembre: «*Redandwhite* me ha dejado plantado y ha desaparecido con mi medio millón». Y eso que no contaba otra cantidad similar que le había ido pagando como adelanto y para gastos. De hecho, todo parece apuntar a que las cinco personas —los cuatro asesinables y el asesino— eran un mismo artista del timo que se aprovechó de la candidez del taimado *mafioso*.

El *Temido Pirata Roberts* no era un programador. Había aprendido por su cuenta. Así, era capaz de montar sitios web funcionales, pero con gigantescos agujeros de seguridad. Algunos *hackers* bienintencionados le avisaron de aquellos que iban descubriendo, pero no todos fueron tan amables. En mayo de 2013, por ejemplo, sufrió un intensivo ataque de denegación de servicio que desconectó la página durante casi una semana. Acababa de abrirse Atlantis, una página que era directa competencia, así que en los foros se especuló durante mucho tiempo con la posible relación entre ambos hechos. Todo el que no pudiera acceder a Silk Road compraría o vendería en su nuevo rival y tal vez no volviera al original. Cuando la agresión terminó, no obstante, el flujo de transacciones continuó a buen ritmo y la cuenta de Bitcoins de Ulbricht siguió aumentando.

Había alguien más buscando agujeros de seguridad, el equipo de cibercrimen del FBI de Nueva York. Una página web moderna no está compuesta de un solo proceso, sino de muchos, y a todos les mandaban peticiones. Tal vez alguna estuviera mal configurada. Se crearon decenas de usuarios, intentaron acceder con datos erróneos, se metieron hasta en el último rincón buscando esa IP que no perteneciera a la Red oculta. Estaban desesperados. Nada funcionaba. Cada resultado que obtenían pertenecía a un nodo de TOR… hasta que el 5 de junio de 2013 les sonrió la suerte, esa que está del lado de quien persevera. Silk Road, como tantos otros sitios web, tenía un sistema llamado *captcha* para evitar que se «colasen» programas de

recopilación masiva de datos. En él aparece un texto o una serie de números que el usuario humano debe reproducir en un campo *ad hoc* para que se le permita el acceso y que se supone que los robots son incapaces de hacer. Por un error de programación, esa comunicación se realizaba de forma directa entre el ordenador destino y el servidor origen, sin pasar por el *enrutamiento cebolla*. Así consiguieron saber dónde estaba el lugar desde el que se coordinaba el que era entonces el mayor negocio ilegal de Internet: un servidor en Islandia en una empresa (centro de datos o, en inglés, *datacenter*) llamada Thor, como el dios nórdico. Por supuesto, Ulbricht jamás habría puesto un pie allí, pero fue el descubrimiento más importante para encontrarlo desde la creación del *ciberbazar*. A lo que sí pudieron echarle el guante fue a una imagen del servidor, bit a bit. Es decir, tenían una copia perfecta de la web y, todavía más, todas las conexiones realizadas durante los últimos seis meses, en especial a la cuenta personal del *Pirata Roberts*, que, por otro lado, solo el día en que la interceptaron había recibido casi veinte mil dólares en comisiones, lo que hacía un beneficio anual estimado de siete millones. A pesar de que había un puñado de conexiones que, por error, también se habían realizado desde fuera de TOR, llevaban a sitios con seguridad adicional, bien *proxies*, bien redes privadas virtuales. Todas salvo una, que conducía a un sitio llamado Café Luna en la calle Sacramento de San Francisco, en California, que llamó la atención de los investigadores de inmediato. ¿Estaría el creador de la web en esa ciudad? Con una sola IP y siendo un lugar público era difícil decirlo. Quizá solo había pasado en una ocasión por allí y vivía lejos.

Los agentes, después de leer mil cuatrocientas páginas de conversaciones privadas de Ulbricht, descubrieron con horror los cinco asesinatos que había planeado y que inicialmente creyeron ciertos, al menos el primero, que incluía documentación gráfica, ya que desconocían la identidad de *Nob* y de su grupo de Baltimore.

Los delincuentes solo tienen que cometer un error para ser atrapados y el *Temido Pirata Roberts* empezaba a tener un listado demasiado largo. El peor de todos, sin embargo, fue el primero que cometió y en el que nadie había reparado todavía hasta que un agente de Hacienda recordó a un tal *Frosty* que había investigado en el pasado por otro caso y lo comentó con la gente del FBI. Resultaba que todas las conexiones de Silk Road estaban encriptadas por alguien que se hacía llamar *Frosty@frosty*.

El Tesoro había detectado que alguien que se hacía llamar *Altoid* había preguntado sobre cómo utilizar en TOR el lenguaje de programación PHP. Ese alias estaba asociado al correo electrónico *rossulbricht @gmail.com* —el nombre y apellido del hasta entonces desconocido *hombre de negocios*—. Poco después, cambió el apodo a *Frosty*. Su fallo había sido el mismo que el pederasta español *Nanysex* del que hablamos en el primer capítulo, un mensaje cuando nadie le conocía y que probablemente ya había olvidado. Pero Internet lo recuerda todo.

Fue fácil encontrarlo en redes sociales y en foros de activismo libertario. Sus ideas y su retórica, y hasta los giros idiomáticos, eran tan parecidos a los del *Pirata Roberts*, que parecía impensable que no fuese la misma persona. Incluso residía en

San Francisco (California), cerca del Café Luna, tras mudarse desde su natal Austin, en Texas. Un nombre, no obstante, no es una prueba de nada, así que tocaba demostrar que manejaba los hilos del mercado negro. Con esa idea en mente, para allí fueron los ciberagentes, encabezados por Chris Tarbell, a coordinarse con la oficina local del FBI, que no entendía demasiado lo que se traía entre manos y pretendía trabajar según el manual y nada más. De momento, varios equipos de paisano lo tenían controlado las veinticuatro horas del día. Nada que ver con las películas. No había una llamativa furgoneta aparcada delante de su puerta ni señores con traje negro.

Descubrieron, además, que el Servicio de Seguridad Interior lo había investigado hacía poco tiempo porque alguien había remitido a su domicilio pasaportes falsos que, como era de esperar, alegó que no eran suyos. Mintió. Era otro consejo de *Nob*, que seguía tratando de quedar con él en persona, para que estuviera listo para desaparecer si sentía que la policía estrechaba el círculo. El agente de la DEA se había ofrecido para moverlo a un sitio seguro, confiando en por fin engañarlo.

Además de detenerlo, para que la operación fuese exitosa de verdad, había que quitar del acceso público el servidor de Islandia y una copia del mismo ubicada en Francia… y nada de eso serviría si no se le podía atrapar con el ordenador abierto y operando. La mayoría de delincuentes de ese nivel lo tienen todo encriptado y lo de adivinar las contraseñas con pequeños trucos basados en lo que conocen del personaje es algo que funciona en las películas, pero no en la realidad. Dependiendo de su habilidad informática, puede ser más o menos difícil conseguir los datos, pero estamos hablando de semanas en el mejor de los casos y de siglos en el peor, y eso disponiendo de equipos y personal muy especializados. Hasta la estimación más optimista no servía, puesto que si no conseguían intervenir la cuenta del *Pirata Roberts* en Silk Road abierta en el ordenador de Ulbricht, todo el caso y el posible desmantelamiento del mercado negro se vendrían abajo. Por eso, se decidió que el día de la operación uno de los hombres de Tarbell, que le había ganado la suficiente confianza como para que mantuviesen charlas a través de TOR, hablaría con él todo el rato. Así se podrían asegurar de que lo tendría abierto.

El responsable local, sin embargo, no entendía las sutilezas que una operación así representaba y había dispuesto que equipos de asalto entrasen por la puerta principal con arietes y armados hasta los dientes. Innecesario y, peor aún, arruinarían el operativo. Bastaba con que Ulbricht bajase la tapa de su portátil para que todo quedase fuera del alcance del FBI. Los ciberagentes no consiguieron hacer razonar a sus colegas, a pesar de la vehemencia y hasta desesperación de sus alegaciones. El día de autos se había programado para el 3 de octubre.

Dos días antes, Tarbell y su gente se encontraban reunidos cerca de un café que solía frecuentar su objetivo, cuando, de repente, se sorprendieron al verlo acudir, con su portátil debajo del brazo. Los agentes se dispersaron, con la poca maña que se dan quienes no están especializados en seguimientos. Por fortuna, Ulbricht tampoco era

un delincuente al uso y la maniobra le pasó desapercibida. Buscó sitio en el local, pero no lo encontró, así que cruzó la plaza y entró a la biblioteca pública Glenn Park, que se encontraba justo enfrente. La ocasión la pintan calva, así que decidieron realizar la detención en ese momento, en cuanto estuviera navegando por Silk Road. Se comunicó a todos los implicados. Los equipos de asalto, con todos los jefes locales, cogieron carretera. Hasta que llegasen, Tarbell estaba al mando y tenía una idea clara: si había que elegir entre el portátil operativo y arrestar al tipo, debían decidirse por lo primero, sin lugar a dudas. A él se le podría atrapar más tarde, pero solo había una oportunidad de tener la prueba de todos los delitos. Los agentes de seguimiento dieron el «recibido». Estaban presentes en la biblioteca, para sorpresa de los ciberespecialistas, que no los podían distinguir entre los presentes. Uno de estos últimos tenía la única función de conseguir el ordenador abierto y nada más.

A las 15.14 del 1 de octubre de 2013, poco después de dar la orden de actuar, una pareja, de mediana edad, con pinta de vagabundos los dos, se puso a discutir justo detrás del objetivo, que giró la cabeza un momento hacia ellos. En ese instante, una joven de rasgos asiáticos y aspecto de estudiante que estaba en la misma mesa de lectura que él, cogió con un gesto rápido el portátil y, en diez segundos, lo puso en las manos del ciberagente que acudía a su misión de arrebatárselo a Ulbricht. Los tres actores pertenecían también al FBI. Un instante después, el fundador de Silk Road estaba esposado. La gente de Tarbell babeaba ante la visión del portátil. Todo estaba a su alcance, la cuenta del *Temido Pirata Roberts* conectada al ciberbazar, las conversaciones, los pagos… Para colmo, estaba configurado como *Frosty*, el nombre que había representado el principio del fin.

El juicio acabó el 29 de mayo de 2015. En él se demostró que Ulbricht había diseñado y dirigido un sitio web destinado a la venta de artículos ilegales, sobre todo droga, opaca a los impuestos, que había realizado en algo más de dos años un millón y medio de transacciones, por los que había recibido un beneficio aproximado del diez por ciento de su valor, esto es, dieciocho millones de dólares en Bitcoins, gran parte de los cuales fueron intervenidos en la redada y vendidos en pública subasta. Fue condenado por una juez de Nueva York a dos cadenas perpetuas consecutivas sin posibilidad de libertad condicional y, además, a otras tres penas de cinco, quince y veinte años, por delitos de tráfico de drogas, lavado de dinero y daños informáticos. De los cinco asesinatos que encargó se libró, porque no se pudo demostrar que las personas que quería matar existiesen en realidad. Un juez de Baltimore todavía debe juzgarlo por el otro homicidio que encargó, el de su antiguo socio *CronicPain*, que fue fingido por la gente de la DEA.

La operación no acabó allí. Los socios del condenado han sido perseguidos allí donde se encontrasen. El 3 de diciembre de 2015 fue detenido el canadiense Thomas Clark, conocido como *Variety Jones*, mentor de Ulbricht y uno de sus principales colaboradores. Se había escondido en Tailandia, donde se encuentra esperando la extradición a los Estados Unidos, acusado de ayudar a organizar y aconsejar en el

desarrollo y operaciones de Silk Road, labor por la que recibió cientos de miles de dólares.

Aún hubo más. El siguiente detenido fue Shaun Bridges, un agente del Servicio Secreto implicado en la investigación en el equipo de Baltimore. Fue uno de los encargados de manejar la cuenta de *CronicPain* tras su arresto y fue quien escamoteó las Bitcoins por las que luego Ulbricht ordenó la muerte de su antiguo socio. Admitió los cargos y fue sentenciado a setenta y un meses de prisión. El siguiente fue Carl Force, el agente de la DEA que se hacía pasar por *Nob*. Se aprovechó de su puesto para realizar pequeñas extorsiones al *Pirata Roberts*, de menos de mil Bitcoins. Por ello pagará setenta y ocho meses en una prisión federal de San Francisco. Después comenzó la cacería de los vendedores de drogas y productos ilegales. A mediados de mayo de 2015 habían salido en prensa al menos ciento treinta y ocho detenciones en todo el mundo relacionadas con la página.

La lucha contra el mercado negro no acabó allí. Casi al mismo tiempo en que desaparecía Silk Road apareció Silk Road 2, que también fue desmantelada poco después, con ochenta y cinco detenidos hasta el momento. Ahora hay decenas de sitios, como Alphabay, en los que se puede comprar y vender casi cualquier cosa como, por ejemplo, datos bancarios, es decir, el dinero de ciudadanos cuyas claves han sido obtenidas de manera fraudulenta. En el capítulo siguiente veremos algunas de las maneras más habituales que tienen las mafias organizadas para conseguirlo. En este vamos a hablar de un caso cuya sofisticación superaba lo habitual.

Un individuo que se hacía llamar *MrBank* (*Señor Banco*) vendía en dos herederos de Silk Road, Alphabay y Nucleus, paquetes que comprendían cada uno una serie de tarjetas de crédito con todos sus datos, incluyendo contraseñas de seguridad y los códigos CCV —esos tres o cuatro dígitos que hay en la parte posterior de los plásticos—. Todos los números pertenecían a una misma entidad española, que se alarmó al ver cómo se disparaba el fraude entre sus operaciones, que llegó a superar el millón de euros en poco tiempo. Ese dinero era cargado en primer lugar a los incautos clientes, si bien luego el emisor tenía que hacerse cargo. Otros dos millones fueron bloqueados por los propios sistemas de seguridad del banco. Los clientes del vendedor estaban más que satisfechos; su valoración superaba el noventa y ocho por ciento en más de cinco mil transacciones —cinco mil paquetes de tarjetas vendidos —, lo que le reportaba pingües beneficios en forma de Bitcoins.

Tras la denuncia en la Unidad de Investigación Tecnológica de la Policía Nacional, los expertos en seguridad lógica empezaron a trabajar. En colaboración con los técnicos de la entidad atacada, detectaron que en el servidor principal del banco se había instalado un programa malicioso —lo que se conoce en el argot como *backdoor* o «puerta trasera»— que le daba pleno acceso al almacén de tarjetas de crédito. Las sospechas recayeron de inmediato sobre alguien de dentro de la empresa. Con los niveles de protección que tienen los bancos era imposible que hubieran podido llegar a través de Internet. ¿Sería alguno de los que estaban ayudando a la policía? Una vez

encontrado, el agujero no era de una sofisticación especial. Usaba un programa comercial como Teamviewer, que está pensado para poder manejar de manera remota un equipo informático, algo que resulta muy útil, por ejemplo, para que el servicio técnico de una empresa no tenga que estar moviéndose por las diferentes sucursales para los incidentes más habituales.

La conexión había de ser bidireccional. Es decir, se tenían que poner en contacto las dos IP, la de la entidad y la de quien quiera que ostentase la identidad de *MrBank*. Por tanto, bastaba con esperar a que se conectase de nuevo y ver a dónde circulaban los paquetes de información. Cuando lo realizó, no sin mucha sorpresa se descubrió a un hombre de veintisiete años que trabajaba, no para el banco, sino para una empresa informática que estaba realizando el mantenimiento y actualización del *software* bancario. Esto se llevaba a cabo por partes. Los informáticos realizaban la programación correspondiente que luego se enviaba al servidor para reemplazar la antigua. En varios de estos envíos, el presunto autor intentó colocar su espía hasta que en una de ellas lo consiguió. A partir de ahí comenzó la extracción de datos y su venta.

Como en el caso de Ulbricht, conocer su nombre no era suficiente. Hacía falta encontrar más pruebas. Por ello, con autorización judicial, la policía decidió, por primera vez en España, emplear sus propias armas contra él y, por la misma conexión por la que robaba al banco, enviaron un troyano que les permitió monitorizar cada acción que llevaba a cabo en su ordenador. Así pudieron ver que, en efecto, conectaba a TOR y se metía en Alphabay y Nucleus como *MrBank*, donde colocaba los paquetes de tarjetas, por los que recibía numerosas Bitcoins cuando las vendía. Con todas esas evidencias, la culminación de seis meses de investigación llegó con una entrada y registro en su domicilio en la que se intervinieron tres teléfonos móviles, cuatro portátiles y ocho unidades de almacenamiento… y *MrBank* quedó fuera de circulación.

Aunque utilizaba TOR para sus negocios ilegales, no podía usarlo para obtener los datos del banco, por lo que resultaba vulnerable. La Policía Nacional buscó una vez más la forma de sobreponerse al anonimato de la *deep web*. Como es habitual en estos delincuentes y el agente Tarbell del FBI sospechaba del dueño de Silk Road, los portátiles se encontraban encriptados. Los mejores expertos de nuestro país siguen trabajando en ellos en 2016.

COMPRAR FAMA, AL ALCANCE DE CUALQUIER BOLSILLO

Las redes sociales son un escaparate ante el mundo, que puede mostrar hasta el último detalle. Cualquier personaje público es destripado sin piedad si comete el mínimo error. Basten los ejemplos del actor Toni Cantó cuando era diputado de UPyD que, entre otras, avisó en 2013 de la muerte de Albert Hoffman, creador de la

peligrosa droga LSD… que había ocurrido en 2008; o de la exparlamentaria del PP Cayetana Álvarez de Toledo que mostró su disconformidad con la cabalgata de reyes de 2016 en Madrid con un *tuit* tan infantiloide y pueril que desató de manera inmediata y viral la burla de miles de personas hasta acaparar portadas de la prensa seria y minutos de los informativos de televisión.

También las empresas, para tener éxito, necesitan una presencia intensiva en las redes sociales, equivocarse poco y mantener una esmerada atención al cliente, sobre todo el insatisfecho. Las amenazas poco veladas o entrar en batallas verbales son un camino seguro al desastre. Incluso la ausencia es observada y analizada con detenimiento.

Muchos personajes necesitan popularidad para que su trabajo se considere más efectivo, y no siempre es fácil conseguirla. Incluso cuando lo es, existe la tentación de aumentarla a base de billetera, aunque sea para superar al rival, algo muy típico entre políticos. Es sencillo encontrar en Internet sitios donde por diez euros se consiguen mil *amigos* más de la noche a la mañana, con rebajas si la cantidad aumenta. Estos seguidores de baja calidad son detectables con facilidad. Suelen estar ubicados en lugares como China o Rusia, creados por robots, sin imagen de avatar y, a menudo, sin seguidores propios (es decir, siguen pero no son seguidos). Son detectables con suma facilidad, incluso sin recurrir a páginas que localizan a estos *bots* como *https://fakers.statuspeople.com/Fakers/V/1*. Se pueden comprar sin ser el usuario legítimo de la cuenta que va a crecer, como forma barata de desprestigiar al contrario o tal vez como una manera equivocada de hacer un favor a quien se admira. Estas adquisiciones, aunque son de ética cuestionable, no son ilegales y la policía no actúa contra ellas. Sin embargo, sí contravienen las normas de Twitter, por lo que tan fácil como vienen, desaparecen y sin que haya lugar a reclamaciones. A finales de 2014, la empresa del pajarito azul eliminó dieciocho millones de cuentas falsas y, por ejemplo, el cantante Justin Bieber, ídolo de adolescentes, perdió un millón de golpe. Por supuesto, él, con setenta y tres millones, no necesitaba pagar para tener un uno por ciento más. Más descarada fue la compra que alguien llevó a cabo para apoyar a Mariano Rajoy, entonces presidente del Gobierno, en 2014. En menos de veinticuatro horas, el 5 de septiembre, ganó casi sesenta mil nuevos seguidores a sumar al poco más de un millón que tenía. Algunas de estas cuentas hablaban árabe o hindi y sus fotos de perfil parecían cogidas al azar de Internet. En cuanto el escándalo saltó a la prensa, el equipo que manejaba la cuenta presidencial se apresuró a buscarlos y eliminarlos con la mayor diligencia. Aun así, según la herramienta de análisis Top Position, hasta el sesenta por ciento de los seguidores del mandatario podrían ser falsos, mientras que Albert Rivera, de Ciudadanos, es el político de primer nivel con menos, en torno al diecisiete por ciento.

Más sofisticada —y, con seguridad, más cara— fue la estrategia montada para apoyar al diario *La Razón* y al Partido Popular a través de una serie de hasta ciento veinte *bots* que fue eliminada por Twitter en agosto de 2015, menos de dos meses

después de entrar en funcionamiento.

A principios de julio, tres personas, que manejaban las cuentas reales *@pplatteau_*, *@_eminence_* y *@_madeinspain_* crearon más de un centenar de otras, controladas por ellos y gestionadas por programas informáticos, que se dedicaban a *retuitear* ciertos mensajes. La mayor parte de lo que compartían eran noticias tecnológicas, a menudo en inglés, y solo una de cada veinte o de cada treinta estaba relacionada con aquellos a quienes deseaban favorecer. Los *tuits* importantes quedaban ocultos entre el *ruido* de los mensajes sobre informática.

¿Qué conseguían con esto, si las cuentas-robot estaban pensadas para pasar desapercibidas? Daban más relevancia a las empresas y personas a las que ayudaban. Según los algoritmos de la red social, es más importante un mensaje que ha sido compartido doscientas veces que uno que lo ha sido apenas diez. Mientras estuvo activa la trama, la portada del periódico objetivo era *retuiteada* cada día por todos ellos. En ocasiones, hasta el cien por cien de la fama de un mensaje se debía tan solo a la actividad de estos *bots*. Esto se notaba en especial en los mensajes que ponían el director del citado diario, Francisco Marhuenda, o destacados miembros del PP. Algunos mensajes entre los tres administradores, los únicos *humanos* detrás de todo esto, elogiaban lo bien que funcionaban los programas que habían desarrollado para controlar a su *horda*, que de alguna manera habían encastrado dentro de dos programas, Hootsuite, que permite programar en qué momento se desea publicar —es decir, no es necesario estar delante del ordenador o teléfono, sino que se pueden dejar redactados y elegir un momento futuro— y Twitter for Android, que sugiere que utilizaban ese tipo de teléfono móvil para ello. Cometieron un error el 25 de agosto, cuando toda esa red criticó al mismo tiempo la cuenta de la alcaldesa de Madrid, Manuela Carmena, con el mismo texto en un periodo de tiempo demasiado corto para que hubiera podido ser viralizado. Esto puso sobre aviso a los responsables de la red social en España y a la gente de *@BotsPoliticosNo*, que hicieron un exhaustivo estudio sobre el funcionamiento del contubernio. Al saberse descubiertos, intentaron redirigir su actividad y comenzaron a aparecer mensajes de apoyo, entre otros, al diario *ABC*, pero ya era demasiado tarde porque Twitter eliminó todos los bots el día veintiocho.

Es difícil saber quién estaba detrás, más allá de ver que eran tres personas diferentes que parecían residir en Madrid y que una de ellas parecía tener acceso a la propia cuenta de *La Razón* en Internet, puesto que los otros le avisaban cuando había algún error en sus mensajes. Como no se cometió ningún delito sino tan solo una infracción de las normas internas de la web, no hubo ninguna investigación y quedarán en el anonimato, tanto ellos como las personas y las cantidades económicas, si las hubo, que se hayan pagado.

EL MERCADO NEGRO COTIDIANO

La mayoría de internautas ha descargado alguna vez un programa, música o película sin pagar por ello cuando deberían haberlo hecho. Incluso los sistemas operativos que funcionan en más del cuarenta por ciento de los ordenadores españoles han sido pirateados. En 2010, todavía en dos de cada diez tiendas de nuestro país se podían obtener Windows falsificados. Para el caso del paquete de ofimática más habitual, el Office de Microsoft, las copias ilegales se acercaban a tres de cada cuatro. La situación en otros sectores es dramática. En 2011, solo dos de cada cien canciones fueron compradas, como la mitad de los videojuegos y los libros, y una cuarta parte de las películas.

El abuso de las obras de propiedad intelectual ha sido una constante en España, de la que ya se quejaban los autores del Siglo de Oro. En la segunda parte de *El Quijote*, Cervantes ataca sin piedad el plagio que había hecho de su obra un tal Alonso Fernández de Avellaneda, que publicó una continuación de la novela original, tomándole prestados todos los personajes. Por supuesto, el veterano de Lepanto no recibió nada por ese mal uso de su trabajo intelectual. Era solo la punta del iceberg, la que ha llegado a nuestros días. Hubo muchas más imitaciones que no llegaron a coger la fama de la aquí mencionada.

Peor lo tenían los autores de teatro, como Lope de Vega, Tirso de Molina o Calderón de la Barca; en los corrales de comedias de toda España se representaban sus escritos sin que ellos fueran siquiera conscientes de ello, ni, por tanto, pudieran salir de la miseria que a muchos acosó toda la vida.

La situación solo mejoró doscientos años después, a finales del siglo XIX, cuando los escritores Sinesio Delgado, Carlos Arniches y los hermanos Álvarez Quintero, entre otros, y varios compositores crearon la Sociedad de Autores de España para protegerse de esos abusos. En 1941 obtendría sus siglas actuales SGAE, que entonces significaba «Sociedad General de Autores de España».

En la segunda mitad del XX, la popularización del magnetófono y la cinta asociada a él supuso que cualquiera podía copiar un disco y pronto los chavales se prestaban los LP entre sí para ello. Las fotocopias eran un proceso más lento y a veces más caro que el original. Aun así, miles de libros fueron duplicados en las reprografías de toda España.

El problema de verdad llegó con Internet. Al principio las conexiones eran tan lentas que incluso ver una fotografía podía llevar minutos, por lo que intercambiar películas era una entelequia. En ese panorama primigenio apareció el concepto de *warez*, donde las cuatro primeras letras provienen de la palabra *software*, o sea, programas de ordenador y la última le daba un aspecto oscuro y marginal, como de pronunciación de bajos fondos que, de hecho, es lo que era. En esa época de finales de los noventa, conseguir copias de herramientas informáticas era, sobre todo, un desafío. Los *crackers* se devanaban los sesos para conseguir el algoritmo que generaba las claves que permitieran utilizar la aplicación que intentaban *reventar* o manipular la programación para que ese requisito no fuera necesario. Luego ponían

esos conocimientos a disposición del público en diferentes sitios hasta llegar a páginas web que llegaron a convertirse en buscadores parecidos a lo que hoy es Google, como *Astalavista.com*, que parodiaba el nombre del que entonces era el rey, Altavista.

La velocidad de la transmisión aumentó y llegó el formato musical por excelencia, el mp3, que comprimía los archivos tradicionales en un tamaño mucho más discreto sin por ello perder calidad apreciable al oído humano. Pronto cualquiera pudo *ripear* —esto es, convertir sus canciones en archivos mp3 para el ordenador— en su casa el CD que se propusiese sin ninguna preparación especial y así la industria de la música cambió para siempre. La venta de álbumes físicos se ha convertido en algo residual. Hoy, la inmensa mayoría de la música se ofrece en descarga para ordenadores, como la célebre iTunes de Apple, en programas patrocinados con publicidad o de suscripción, como Spotify, o los canales del portal de vídeos YouTube, donde sobresale Vevo.

Los discos fueron los primeros en sufrir el varapalo que les forzó a reconvertirse o desparecer. Luego llegaría la bofetada a los audiovisuales —películas y series—, que supieron capear mejor el temporal, al menos en los Estados Unidos y, por último, a los libros, con la explosión de los lectores de tinta electrónica, algo que pilló a contrapié a casi todas las editoriales en España y que en 2014 arrojaba datos de que una de cada dos obras escritas era descargada sin pagar por ello. Los que mejor se adaptaron desde el principio fueron los videojuegos, cuyos nuevos productos estaban orientados, sobre todo —a veces en exclusiva— a jugarse *online*, dentro de los servidores de la propia empresa, que podían detectar al instante cualquier pirateo. Algunos incluso pueden descargarse gratis, aunque hace falta pagar una cuota mensual si se quiere disfrutar de verdad. Eso, sumado a ofertas en plataformas en Internet, como la popular Steam, que pueden llegar al ochenta por ciento del precio original, han hecho que hayan impulsado hacia delante el desarrollo de las tecnologías asociadas.

Los primeros piratas, antes de Astalavista, no tenían páginas donde alojar sus contenidos ni existían todavía los programas *peer to peer*, que sirven para compartir contenido entre iguales. Estos pioneros utilizaban el IRC que ya comentamos en el primer capítulo, los famosos *chats*. Mediante unos pequeños programas llamados *scripts* ponían una parte de su disco duro a disposición de otras personas que entrasen al mismo canal. Con un proceso automatizado, cada «visitante» tenía que entregar algo a cambio de lo que se llevase. En algunos casos, el trato era uno por uno; los más generosos llegaban al cuatro por uno. Había que conocer los comandos para saber navegar por el disco duro objetivo y para elegir qué descargar y cómo enviar. Era todavía un medio relativamente minoritario. Preocupaba, sin desatar la alarma que pronto llegaría. Descargar un sistema operativo, por ejemplo, requería demasiado tiempo de conexión para ser viable en la mayor parte de los casos. Para eso se recurría a las grabadoras de CD y más tarde de DVD que se popularizaron en el

cambio de siglo. Quien tenía algo que otro deseaba, se lo copiaba y, en muchas ocasiones, se lo vendía, desde música hasta juegos pasando por todo lo imaginable.

El verdadero caos comenzó con Napster y estallaría con la segunda y tercera generación de programas *entre iguales*. En vez de complicados comandos y que cada persona solo compartiese lo que almacenaba, ¿por qué no crear una red en la que todos los que participen compartan lo que desean y, mejor todavía, que todos los que tengan un mismo archivo puedan compartirlo con todos los que lo deseen a la vez? Es decir, cada persona que desea un contenido determinado, puede descargárselo *al mismo tiempo* de todos aquellos que lo posean. Sin necesidad de servidores, de páginas web ni de nada más que los propios sistemas de búsqueda creados dentro de estas aplicaciones. El crecimiento fue exponencial. En pocos años, una gran fracción de los internautas se estaba descargando contenido protegido.

Que los internautas compartan contenido protegido entre ellos no es buena manera de conseguir dinero. Si acaso, lo es para los delincuentes que llenaron de virus aquellas redes para conseguir robar los datos bancarios o de cualquier otro tipo de sus víctimas. Demasiado complicado y poco ético para la inmensa mayoría de *emprendedores con lo ajeno*. Alguien tuvo una idea poco después que creció como la espuma: ¿por qué no montar una web que diese a conocer los enlaces donde se podía adquirir música o películas? Los propios archivos estarían almacenados en los ordenadores de los particulares. Ellos solo les pondrían en contacto entre sí. Poca capacidad de almacenamiento pero mucho tráfico. Eso también es caro. ¿Y el negocio? La publicidad *online*. Por cada persona que visitase al anunciante de una de esas webs sus dueños ingresarían algunos centimillos. Eso multiplicado por cientos de miles de accesos representaba una pequeña fortuna. Quien se cree más listo que nadie por no pagar por lo que antes lo hacía en el videoclub no está dispuesto tampoco a enriquecer a su pirata particular, así que comenzó una guerra que aún se mantiene para engañarlo, con botones falsos de acceso a los enlaces, ventanas emergentes que se cruzan en el camino del ratón, *banners* —nombre que reciben los anuncios incrustados en una web— engañosos… y todo cuanto diera de sí el ingenio del ser humano.

El reinado de los *peer to peer* no duraría mucho, sustituido por otra forma de descarga más obvia, la directa. Los contenidos están de hecho alojados en lugares físicos. En Internet, el tráfico cuesta dinero y el de muchos *megabytes* —el alojamiento de una película— es más caro que el de unos pocos *bytes* —un enlace—, así que necesitan más ingresos. Para financiarse y lucrarse, además de la misma publicidad anunciada anteriormente, también ofrecen un sistema de suscripción que el pirata doméstico ha estado más dispuesto a pagar —dentro de la marginalidad— que a quien posee los derechos de explotación. Estas páginas comenzaron con la alemana Rapidshare que se vio obligada a modificar sus condiciones y a restringir de forma drástica el acceso a sus servicios. Al contrario que otras, estaba pensaba para que las empresas y particulares pudieran compartir de forma rápida documentos que

por su tamaño no se podían enviar por otros sistemas, como el correo electrónico. Luego llegó Megaupload, del magnate alemán afincado en Nueva Zelanda Kim Schmitz, conocido como *Kim Dotcom*, que se podría traducir por Puntocom en referencia al dominio de primer nivel más popular. Después, incontables clones: Rapidgator, Uploaded, Netload y un largo etcétera. Los enlaces se almacenaban en foros, mantenidos con los aportes de sus usuarios para el enriquecimiento de los dueños o en los mismos sitios que antes tenían datos para la descarga P2P, donde a menudo ambas opciones se solapan incluso hoy.

En un paso más allá, estos piratas voluntarios que ponían contenidos en foros intercalaron unas páginas publicitarias entre el foro y el sitio de descarga, de manera que ellos cobraban también por visita. En el colmo del paroxismo, estos individuos iniciaban diatribas indignadas cuando, a su vez, alguien ofrecía gratis el mismo contenido que ellos. Eran habituales expresiones como «si vuelvo a encontrar mis escaneos en eMule —uno de los más conocidos sistemas P2P— dejaré de hacerlos. ¿Quién me paga a mí los tres euros de la revista?». Preguntarse por quién pagará a la gente que, de hecho, intenta ganar su sueldo haciendo esa revista de la que él se aprovechaba estaba más allá de su capacidad de empatía.

Nadie estuvo a la altura, ni la industria, ni el gobierno, ni los consumidores responsables, menos aún en España. Mientras en Estados Unidos o Japón la ilegalidad está en torno al veinte por ciento, en España, en el mejor de los casos está en más del doble. Solo Italia nos supera por poco en la clasificación europea. Para entenderlo hay que tener en cuenta varios factores. Uno de ellos es el cultural. Lo que en el país nipón es impensable —apropiarse del trabajo de otro—, aquí no: quien defrauda a Hacienda es el más listo de su barrio y hasta alardea de ello. El segundo factor es la legislación más o menos restrictiva, que hay que entroncar con el primero; y es que no se puede criminalizar un comportamiento que está tan arraigado. No se puede convertir a toda la población en ilegal.

Aquí llega el tercer factor, ofrecer al ciudadano contenidos a un precio aceptable y de una manera rápida. Darle una opción válida. El modelo tradicional se ha visto sobrepasado y casi aniquilado. Sin embargo, quien se ha sabido adaptar, sobrevive. El ejemplo paradigmático es el videoclub virtual Netflix. Unos datos tan bajos de copia audiovisual en el país de las barras y estrellas se explica cuando por apenas ocho dólares al mes, cualquiera tiene a su alcance casi todas las series y películas en alta definición, con sonido envolvente y disponible cuando lo desee ver. Un estudio realizado en Australia —un país con poca incidencia de piratería, en torno al veintinueve por ciento— por la IP Awareness Foundation ha mostrado que, en un solo año desde la implantación del negocio, estos índices han caído cinco puntos. El consumidor medio prefiere pagar y tener el servicio a su disposición que tener que buscar en sitios fraudulentos, ser engañado y a veces llevarse sorpresas desagradables: hubo un tiempo en que era normal buscar una película y encontrarse con las desagradable realidad de descargar pornografía, a veces de menores.

Otros modelos editoriales también están teniendo éxito. Dejando a un lado el sistema Amazon, que en ocasiones lleva a cabo prácticas cercanas al monopolio, con penalizaciones a quien no entre por su aro, en nuestro país triunfa la empresa Lektu para la venta de libros electrónicos. Una de sus principales normas es que no cree en los medios de protección anticopia que la mayoría de otros negocios del sector incluye. Son ineficientes y, además, causan serios problemas al lector con escasos conocimientos de informática. Lo que triunfa es lo sencillo y ellos lo han entendido muy bien. Incluso hay escritos que se pueden descargar gratis, realizar un *pago social* —esto es, hacer publicidad de lo descargado— o que cada consumidor decida cuál es el precio que considera justo.

En diferentes países se han hecho necesarias modificaciones legislativas —como las que consiguió la SGAE original a finales del siglo XIX— para proteger la intangible propiedad intelectual; si los creadores no pueden vivir de sus obras, no crearán. Sin embargo, no se puede poner puertas al campo. La represión por sí sola no sirve. La famosa ley francesa que preveía incluso el corte del acceso a Internet a los que descargasen contenidos protegidos fracasó por completo, del mismo modo que la Ley Sinde-Wert en España.

El ciudadano que descarga contenidos sin pagar por ello está aquí para quedarse. Es imposible eliminar ese hábito. La responsabilidad de todos está en ofrecer los contenidos por un precio asequible y de una manera sencilla. Así, esa parte del negocio ilegal menguará hasta la marginalidad en la que se encuentran, a pesar de su relativa popularidad, el resto de los negocios *negros* que hemos tratado en este capítulo.

6

LOS PROFESIONALES DEL ROBO

Clancy[2] *no se podía creer lo afortunado que era. Un hombre de mediana edad, feliz en su matrimonio y un afamado dentista en la ciudad canadiense de Toronto. Por si eso fuera poco, acababa de recibir un correo electrónico en que le notificaban que había ganado el máximo premio —conocido como El Gordo— en la Lotería Nacional de un país europeo llamado España. Se consideraba un hombre de mundo y, además, tenía estudios. Sabía dónde estaba esa nación, lo que había sido a lo largo de la historia y hasta recordaba un absurdo conflicto a mediados de los noventa por algún oscuro motivo relacionado con la pesca que en realidad ocultaba una maniobra del entonces primer ministro Brian Tobin para su reelección. En el siglo XXI, España era famosa por dos cosas por encima de las demás, sus fiestas y su afición a los juegos de azar. La absurda cantidad de dinero que le había tocado no estaba fuera de lo normal. En el propio correo le avisaban, eso sí, de que una parte sustancial iba a convertirse en impuestos del país emisor. Lógico. En todas partes pasaban esas cosas. Así, pues, respondió de inmediato para iniciar los trámites y reclamar los millones. La respuesta del organismo emisor no tardó en llegar. Debía enviar unos pocos cientos de dólares o euros, a su elección, en concepto de apertura. Poco después, fueron otros pocos cientos en concepto de tasas para registrar el expediente en la Oficina Internacional de Apuestas del Estado, al ser el destinatario un extranjero. A continuación, unos miles más como primera fase de la transacción. Llevaba pagados dos millones de dólares cuando empezó a sospechar que algo no iba bien. Preguntó a un amigo suyo, abogado, que se echó las manos a la cabeza.*

—Clancy, te han engañado pero bien. ¿No te parece un poco extraño que te haya tocado un premio de una lotería a la que no has jugado?

Asustado y con una sensación de desasosiego en el cuerpo, acudió a la policía, aun pensando que su amigo se equivocaba. Los agentes que le atendieron fueron muy amables y profesionales. Le explicaron los pormenores del engaño. Cómo las mafias del timo en Internet se dedicaban a lanzar millones de correos esperando que algún ciudadano de buena fe picase. ¿Y las posibilidades de recuperar el dinero? Escasas. No obstante, utilizarían los canales de colaboración internacional, en especial Interpol, para ponerse en contacto con sus colegas de la Policía Nacional de España. Ningún seguro normal se haría cargo de la estafa, dado que consideraban que el engaño no era suficiente y que el timado debería haber tomado medidas para no picar.

Un año después, en 2007, le llegaron noticias en cierto modo positivas. Los agentes de la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía habían detenido a varias personas relacionadas con los hechos, desde el receptor

inicial del dinero —la pieza más baja de la organización y a menudo un colaborador indirecto— hasta varios organizadores. Eso sí, del efectivo, enviado a países de Este de Europa en diferentes remesas, nunca jamás se supo.

LA MAFIA QUE NO SE CONOCE

Ser rico es la meta de mucha gente. Conseguirlo de forma legal es complicado —por decirlo suave—, así que la tentación de utilizar otros caminos es muy alta entre aquellos que respetan poco las leyes y a su prójimo, porque la forma más sencilla de obtener dinero es quitárselo a otros. Desde el robo callejero a punta de navaja hasta los grandes desfalcos en los bancos, las maneras son muchas. Pocas presentan una relación riesgo/beneficio tan baja como las estafas por Internet, en especial aquellos que se aprovechan de la buena fe de la gente —o, a la manera del timo tradicional, como el tocomocho o la estampita, de aquel que se pasa de listo—. Con muy poca inversión y poca exposición personal, se consiguen unos beneficios relativamente altos.

Aunque es llamada «mafia» de forma popular, su forma de actuar es del todo diferente a lo que se entiende por ese nombre, con vínculos muy íntimos y normas que seguir a rajatabla, como la tradicional siciliana o sus adaptaciones estadounidenses que se hicieron famosas durante los años veinte, con Al Capone y su Sindicato del Crimen como paradigma de todos ellos. Las de Internet no necesitan tener un código de silencio porque, de hecho, la mayoría de ellos no se conoce entre sí. Algunos en los escalones finales de la cadena ni siquiera son conscientes de que están trabajando para el crimen organizado. Porque, de eso no cabe duda, sus acciones encajan con las instrucciones de la Unión Europea y de la Fiscalía General del Estado, que definen diez indicadores de ese tipo de crimen, de los que al menos seis deben cumplirse:

1. Existencia de un grupo de personas más o menos numeroso.
2. Reparto de tareas o de papeles entre los miembros del grupo.
3. Actuación prolongada en el tiempo o indefinida.
4. Comisión de actos delictivos graves.
5. Actuaciones transnacionales o intensa movilidad territorial dentro del estado.
6. Uso sistemático de la violencia o de la intimidación grave.
7. Utilización de instrumentos jurídicos legales para crear estructuras económicas o comerciales.
8. Actividades de blanqueo de capitales.
9. Influencia sobre cargos públicos o personas que desempeñen su función en la esfera política, medios de comunicación social, funcionarios de la Administración Pública y/o de la Administración de Justicia o sobre la actividad

económica mediante la corrupción.
10. Finalidad primordial de obtención continuada de beneficios económicos o de cualquiera de las diversas formas de influencia política, social o económica.

Los grupos que vamos a analizar en este capítulo cumplen todos salvo el sexto. Los más básicos o simples tampoco encajan en el séptimo y el noveno. En las estafas por Internet, además, es muy significativo el punto quinto. Como veremos, los delincuentes suelen estar en varios países al mismo tiempo, sin más relación entre ellos que la estricta *laboral*. Poco pueden contar unos de otros y esa, entre otras, es la base de su éxito.

A la hora de empezar a delinquir, una persona o pequeño grupo tiene la idea. A menudo han sido miembros en puestos inferiores de otros grupos similares ya desaparecidos —por acción policial o simple cambio de intereses—. Conocen una pequeña vulnerabilidad —bien sea informática o, más a menudo, humana—, y desarrollan una forma de explotarla. Estos jefes o directores organizan toda la trama y reparten los diferentes papeles que deben asumir los demás miembros, a los que reclutarán en diferentes lugares según la importancia que vayan a tener dentro de la organización.

El siguiente eslabón son los programadores. Es necesario un grupo de expertos informáticos que escriban el código adecuado para explotar el error. Dependiendo de la especialidad, el número será mayor o menor y deberán conocer un lenguaje informático u otro. Los timos más sofisticados requieren a los más especializados y más difíciles de reemplazar. Estos profesionales provienen en un cierto número del mundo del *hacking* y la seguridad informática. Muchos son ingenieros jóvenes, recién titulados. En ocasiones, las mafias van a reclutarlos en las propias universidades.

Una vez creada una *criatura* hace falta hacerla llegar a la gente. Ahí entran los distribuidores masivos. Desde el nacimiento de Internet, el medio preferido para ello ha sido el correo electrónico. Ahora, en la segunda década del siglo XXI van entrando otras opciones, como redes sociales, mensajería instantánea —por ejemplo, WhatsApp—, llamadas telefónicas o cualquier otro método barato de llegar a muchas personas. Los listados de correos electrónicos se compran y se venden de forma más o menos legal. Existen empresas ajenas a la estructura criminal —el equivalente a una subcontrata en los negocios lícitos— que se dedican a recopilar información válida de clientes —o futuros timados—. En el caso más típico, el de los correos electrónicos, esto se consigue de varias formas. Por un lado, existen *bots* programados para rastrear Internet en busca de direcciones válidas. Ahí entran tanto de particulares como todos los de empresas e instituciones que necesitan tenerlo a disposición de sus clientes. Por poner solo un ejemplo, la cuenta de la policía *delitos.tecnologicos@policia.es* recibe decenas de mensajes de timadores cada día.

Por otro lado, están los mensajes en cadena que era habitual recibir en los buzones, algo cada vez más en desuso. Se compartía una foto, una presentación de

Power Point o un simple chiste, que se iba reenviando sin borrar nunca a los emisores originales… que eran quienes recopilaban las direcciones que luego se ponían a la venta sin conocimiento ni autorización de la víctima. Hoy, la versión está en Facebook con los falsos sorteos. Es habitual ver propuestas como «se regalan diez iPhones porque han sido desprecintados y no se pueden vender». Para optar a ello solo hay que darle a *me gusta* a una determinada página. Por supuesto, el concurso no existe y nunca hay ganadores, pero se obtienen decenas de miles de direcciones válidas. Los principales clientes de estos intermediarios recopiladores son otro tipo de negocio pseudolegal, el *spam*, esto es, la publicidad intrusiva no deseada. Otras veces, los dueños de páginas venden los datos de sus clientes. Es habitual, aunque ni muchos menos exclusivo, en foros gratuitos y páginas de descarga de material protegido por derechos de autor. Todas ellas tienen en común que el usuario debe registrarse y, para ello, ha de aportar un *email* válido. La práctica totalidad de usuarios de Internet han recibido alguna vez un correo en que les venden Viagra, Cialis, un alargador de pene o gafas de sol de primeras marcas; todos estos productos son falsos en el mejor de los casos. Somos su objetivo porque nuestra dirección está en alguno de esos listados. Cuanto más tiempo lleve activa una cuenta, más fácil es que acabe en alguno de ellos. Si algún lector quiere hacer la prueba, basta con que deje una dirección que use en algún lugar público de Internet y que cuente los días en que le empieza a llegar más *basura* virtual de la habitual.

Los distribuidores de la organización compran estas listas —ya vimos en el capítulo anterior que un millón de correos cuesta entre trescientos y ochocientos euros, dependiendo de su antigüedad y verificación—. Saben que en torno a un veinte por ciento, como mínimo, serán falsas o ya eliminadas, pero da igual. Su porcentaje de éxito es inferior al uno por mil, así que necesitan grandes números, sin reparar en la calidad.

El siguiente paso es redactar el mensaje gancho, que será diferente para cada variedad. Debe ser atractivo, pasar los filtros de correo no deseado, cada vez más precisos, y estar escrito en el idioma del destinatario. Un correo en francés en España o en español en Brasil tiene una incidencia muy inferior. Así, la organización buscará personas que dominen la lengua del futuro timado. Esto a veces no es tan sencillo como parece y el equipo de redacción se ve forzado a utilizar traductores automáticos que aún están muy lejos de ofrecer una calidad suficiente. Por ello, una de las formas más típicas de detectar una de estas estafas es por su redacción deficiente. Este grupo debe estar en íntimo contacto con el anterior para coordinarse, dado que a menudo el trabajo de uno depende del de los otros. Por ejemplo, los mensajes de una web falsificada deben estar en el idioma correcto y los correos señuelo deben contener el enlace apropiado.

Una vez que empiezan a recibirse respuestas, un grupo de mafiosos debe hacer las funciones del contacto con el *primo* y las gestiones para desplumarle. Según el tipo de estafa, este número será más o menos grande y deberá tener más conocimientos

informáticos o psicológicos. Puede que incluso se le requiera una buena presencia personal o tal vez solo soltura ante un teclado numérico.

Por supuesto, es necesario recaudar dinero. Sin ello, no hay beneficio, que es el objetivo final. Para lograrlo hace falta un sistema que dé seguridad suficiente de que la transacción no pueda ser rastreada. Esta es a menudo la parte que más personal emplea, unos trabajadores que incluso desconozcan que están delinquiendo —aunque, como mínimo, deberían sospecharlo— y que en ocasiones son los necesarios cabezas de turco.

La parte más débil de la cadena, la más numerosa y prescindible es la que se conoce como *mula* o *mulero* en el argot policial. Son reclutados del mismo modo que se busca a víctimas, mediante envíos masivos de correo. En este caso simulan ser una importante multinacional que está buscando a trabajadores en el país correspondiente —el que sea— y a la que deben enviar el currículo lo antes posible. Por supuesto, todos los candidatos son «seleccionados». En siguientes mensajes explican que su función va a ser proporcionar una cuenta bancaria propia en la que irán ingresando dinero —que procede de robar a otros ciudadanos—. El incauto delincuente debe enviar el noventa por ciento de ese dinero a otro lugar, a menudo utilizando sistemas de envío de remesas como Western Union o Money Gram, con lo que se pierde el control del destinatario, y quedarse el otro diez por ciento en concepto de *sueldo*. Cada año son detenidas en España decenas de personas por este motivo. La policía considera que nadie de buena fe puede considerar un empleo serio el arriba descrito, donde no hay un esfuerzo mínimo y los ingresos son considerables. Los jueces suelen estimar que el incauto ha cometido una imprudencia grave en un delito de blanqueo, por el que es condenado. Solo en ocasiones puntuales entienden que el engaño ha sido suficiente y lo han absuelto. En cambio, la acusación de estafa no suele prosperar, puesto que, según el código penal, no existe la figura del imprudente en ese delito. Los mafiosos no suelen recurrir a un mismo mulero más que en una o dos ocasiones, puesto que saben que es vulnerable y la probabilidad de que sea detenido y las transacciones bloqueadas es muy alta. Algunos grupos solicitan que se remita un certificado de antecedentes penales, en el colmo del cinismo. El motivo es que ellos, también, han sido estafados en el pasado por sus empleados. Entre otros casos, en 2006 y 2007 un *mulero* abrió varias cuentas bancarias con documentación falsa por la zona del Levante español. Cuando los mafiosos le contrataban, se limitaba a quedarse todo lo que le enviaban, sin remitirles su parte. Estos grupos no disponen de sicarios —no son necesarios— y, en todo caso, resulta más caro —penal, moral y organizativamente— buscar y asesinar que tener más cuidado con quien se contrata.

Por encima de ellos están los receptores y canalizadores. Las asociaciones más grandes disponen de *gerentes regionales* para controlar a los *muleros*. Suelen tener responsabilidad para todo un país y son los encargados de organizar la manera en que sale el dinero. Algunos dan varios saltos de cuenta en cuenta antes de que lleguen a su destino final, mientras que otros son más directos y se limitan a hacer el envío a

los jefes. En ocasiones, los responsables de dos países se ponen de acuerdo y realizan envíos de remesas o transferencias entre ambos lugares. De esta manera dificultan la investigación, dado que la colaboración transfronteriza en cuestiones monetarias es escasa. Algunos países exigen que el monto sea superior a seis mil euros para empezar a mover su maquinaria legal.

Los receptores de los envíos realizados desde empresas de remesas (las mencionadas Western Union, Money Gram, etc.), tanto si son intermediarios como si son finales, si no están en connivencia con alguien de la sucursal, utilizan a personas sin hogar o con especiales necesidades económicas para que retiren los fondos, a cambio de una comisión miserable —inferior a los cien euros, que en ciertos países puede ser una fortuna—. Si la policía está esperando al delincuente, el único detenido es el contratado para ello. Si no, entregan el dinero en mano y se pierde todo rastro de la transacción. De esta manera, tras un número indeterminado de saltos, los euros acaban en manos de los jefes y el círculo de la estafa se completa.

Por supuesto, no todas las organizaciones deben tener cada uno de estos puestos. Según las tipologías, como veremos más adelante, pueden faltar algunas de ellas o, sobre todo en las bandas más sencillas, varias funciones estar aglutinadas en una misma persona o grupo. Por ejemplo, es habitual que los jefes sean también programadores y que la redacción de los correos y su posterior respuesta a las víctimas la lleven las mismas personas.

En cualquier caso, no existe una sola *mafia rusa*. No es una mega-organización, sino una multitud de entidades que aparecen y desaparecen con el tiempo, a medida que sus miembros son detenidos, abandonan la delincuencia o se establecen por su cuenta. Algunas de estas son capaces de un desarrollo técnico muy sofisticado, con programas de gran calidad, y en otros casos requieren de una buena *colaboración* por parte del *primo*. Además, una vez que un tipo de estafa se hace popular o funciona, otros copian el método. Los más, con un desarrollo más burdo, algunas, sin embargo, mejoran el original. Con la larga historia, aún presente, del conocido como *virus de la policía*, que veremos en profundidad en el capítulo octavo, se pudieron ver desde mensajes que estaban escritos en un español bastante defectuoso hasta otros que eran perfectos hasta en el uso de los emblemas policiales —en uno de ellos incluso utilizaron una foto de este autor vestido de uniforme que había salido en prensa—. En cuestión de programación, algunos encriptan todos los archivos de un ordenador para forzar a efectuar un pago que no garantiza su liberación, mientras que otras variantes que siguen apareciendo tiempo después de la detención de sus creadores apenas bloquean la pantalla del navegador, algo que un usuario medio de Internet puede arreglar con un mínimo esfuerzo.

Como hemos contado, los miembros de las organizaciones a menudo no se conocen entre sí. Para comunicarse suelen utilizar métodos seguros de la *deep web*. Solo dentro de la red TOR pueden usar el correo electrónico *Tormail* o el sistema de conversación en tiempo real *Torchat*. Ambos garantizan una seguridad suficiente para

no ser detectados. Ya vimos en el capítulo anterior cómo, a pesar de los esfuerzos y recursos de varias agencias policiales de Estados Unidos, no podían ubicar al creador de *Silk Road* ni a sus secuaces mientras usaban estos sistemas.

Sin contar los escalones más bajos —*muleros* y los cobradores que retiran efectivo proveniente de las remesas—, las bandas tienden a estar formadas por personas de la misma nacionalidad, con domicilios dispersos por el mundo —los *gerentes regionales* suelen residir en el país que controlan—. Aunque no hay ninguna nación que se libre de tener a sus propios delincuentes, las organizaciones más tecnológicas suelen ser rusas o ucranianas, mientras que aquellos que requieren más artes personales a menudo están ubicados cerca del Golfo de Guinea, en especial, Nigeria. Los traficantes de números de tarjetas de crédito copiadas tienden a ser originarios del Caribe.

La empresa especializada en seguridad informática Kaspersky, con sede en Rusia, estima que en el año 2015 no había más de veinte personas de su nacionalidad que formaran el núcleo de los grupos criminales. Son los que han detectado accediendo a los foros secretos sobre transacciones ilegales. El resto pertenece a los escalones inferiores o periféricos.

Desde el año 2012 hasta el presente hay tan solo cinco organizaciones activas, que están formadas —sin contar a los *muleros*— por entre diez y cuarenta personas. Ese es el número de delincuentes cuya única labor profesional es engañar y robar a través de Internet. Hace falta, pues, muy poca gente para causar un perjuicio económico multimillonario.

La policía no descansa, porque también en España tenemos nuestras propias organizaciones o parte de otras más grandes. Se trabaja en coordinación a través de Europol e Interpol con las fuerzas de otros países, en especial de Europa. Tan solo en el año 2015 la Unidad de Investigación Tecnológica detuvo a doscientas ochenta personas por estas tipologías.

LA MODERNIZACIÓN DEL TIMO DE LA ESTAMPITA

En los años ochenta, en el buzón del domicilio de muchos particulares de todo el mundo empezaron a aparecer cartas selladas en Nigeria. De ahí el nombre que este engaño conserva hasta hoy en día, *cartas nigerianas*. En ellas se contaba que un príncipe africano había sido derrocado por los rebeldes y que necesitaba sacar su fortuna del país lo antes posible. Como estaba siendo controlado por los revoltosos, necesitaba una ayudita en el extranjero —el afortunado receptor de la misiva— para desbloquear los fondos y hacerse con una indecente cantidad de millones de dólares de los cuales el colaborador podría quedarse un generoso diez por ciento. Hacía falta enviar un giro postal con el que liberar los depósitos bancarios, que serían de inmediato transferidos a su cuenta. A pesar de lo extraño que resultaba todo, una

buena cantidad de españoles mandó sus pesetas al África Occidental y, como era de esperar, jamás volvió a saber de ellas.

La popularización de Internet puso a disposición de los estafadores un mundo de incautos varias millones de veces más grande del que disponían hasta entonces. Y más barato, puesto que cuesta menos —en tiempo y en dinero— remitir un correo electrónico que uno postal. La inversión más importante a realizar son los listados de direcciones válidas. Si se paga lo suficiente, se pueden conseguir hasta por zonas geográficas, para ser más precisos a la hora de utilizar un idioma u otro. Por lo general, el especialista en este delito hace una inversión muy baja, así que los escritos suelen ser traducciones automáticas de pésima calidad.

El proceso se ha alargado en el tiempo respecto a las cartas del siglo pasado. Entonces debían realizar toda la petición en un solo mensaje, con lo que la estafa quedaba al descubierto ante una lectura detallada. Ahora, como en los tradicionales timos, existe el factor humano, el contacto cercano entre el timador y el timado y, por supuesto, la solicitud de dinero no es inmediata.

Este tipo de organización no necesita programadores, así que ese puesto queda sin asignar. Los redactores presentan un mensaje que hace mucho que perdió su originalidad: diversas variantes sobre una viuda que ha heredado una fortuna de su marido y no puede hacerse cargo de ella porque está investigada en su país y necesita que alguien del extranjero la ayude. En otras versiones es un caballero a punto de morir que quiere donar sus millones, bien para obras benéficas y quien le ayude se lleva un buen pellizco o bien de forma directa a tres afortunados elegidos al azar. Otras veces es un soldado en Iraq que ha encontrado millones en un agujero y necesita sacarlo del país o incluso una importante empresa nos propone que vendamos un oro que nos ofrece a un diez por ciento de su valor nominal. Una que tiene especial incidencia en nuestro país es la estafa de la Lotería Nacional, como la que hemos visto al iniciar este capítulo. En un paso más, hay organizaciones que funcionan desde aquí, gestionadas por alemanes que llaman por teléfono a ciudadanos de su país para comunicarles que han ganado algo a lo que nunca han jugado. Las variaciones son tantas como dé la imaginación humana. Todas tienen en común que se ofrece a una persona al azar un negocio inmejorable en el que no tiene que invertir nada.

O casi nada, porque, si contestamos al amable extranjero que nos propone tan generoso negocio, en el siguiente correo ya empezarán con peticiones. Hay un fenómeno psicológico que hace que la mayoría de seres humanos esté deseando recibir noticias positivas en su buzón. La propuesta es tan buena que el *pardillo* piensa que no le van a contestar, puesto que habrán elegido a otro. El grupo de estafadores encargados de gestionar las relaciones con las víctimas responde a todos, y a cada uno le ofrece el mismo ventajoso plan. Lo único que necesitan de la víctima es una pequeña aportación. El motivo variará en función de lo que hayan contado al principio: para impuestos, sobornos o desbloquear los fondos —al tener la viuda

todos sus ahorros congelados no puede pagar la tasa necesaria para recuperarlos—. El intercambio de mensajes es intenso y lo acompañan de recibos falsificados de diversos bancos africanos o del país oportuno. En algunos casos incluso inventan personajes como directores de banco o agentes de aduanas. Utilizan cuentas de correo que simulan ser una entidad financiera que confirma que ha recibido el pago y está transfiriendo los fondos. Todo ficticio. El objetivo es seguir sacando dinero al incauto, a poder ser cantidades más altas y cada vez con motivos más peregrinos. Algunos *clientes* piden una prueba de verosimilitud, saber quién es el que está al otro lado del ordenador. Los estafadores están más que dispuestos a enviar fotografías. Como algunos incautos siguen sospechando, les llegan a pedir que lleven un cartel con un mensaje concreto para así saber que son ellos y que no han cogido la foto de Internet. Sin embargo, algunos de los supuestos primos no son tales, sino cazadores de *scammers* (como se les conoce en inglés) que llevan una verdadera competición para conseguir que les envíen fotografías humillantes. Es fácil encontrar a los timadores vestidos de reno, con ropa de mujer o portando carteles con frases como «me gusta chupar penes», por hacer mención a alguna de las más ligeras y menos ofensivas. Muchos de estos son recopilados en una web llamada *419eater.com* que, además, incluye consejos y una muy útil recopilación de todas las cartas nigerianas de las que han tenido noticia.

Esta modalidad es tan fácil de detectar que incluso los filtros automáticos para el correo no deseado encuentran la mayoría. En cualquier caso, debemos sospechar de cualquier oferta demasiado ventajosa que provenga de un desconocido que nos haya escogido al azar. Peor aún si está mal escrita. Por supuestísimo, jamás hay que enviar ningún dinero a un desconocido, menos todavía a través de medios no rastreables como los que hemos comentado más arriba. En cuanto nuestra remesa, por el medio que sea, sale del país, hemos perdido el control de la misma de forma absoluta.

No difiere mucho, pues, del tocomocho tradicional, que se hacía a pie de calle. Un miembro del equipo de timadores se acercaba al incauto para venderle un billete de lotería en apariencia premiado porque debía abandonar España y no tenía opción de cobrarlo antes de la apertura de la sucursal de Loterías y Apuestas. Un segundo estafador, que fingía no conocer en nada al primero, aparecía después de un rato con una lista de boletos premiados y confirmaba que, en efecto, el número estaba agraciado con una cierta cantidad. Al *pardillo* le desplumaban de todo lo que podían sacarle en el banco y desaparecían. Cuando se quería dar cuenta, ya estaban demasiado lejos. Las cartas nigerianas no son más que la evolución de esto. Ellos, al jefe de un grupo lo llaman *oga* y solo lo conocerán los engañados (*mugu*) que han pasado los primeros filtros de los que trabajan escribiendo y respondiendo correos, los *guyman*.

En ocasiones cae hasta gente a la que se supone suficientes conocimientos de leyes para detectarlos. En 2009 un empresario español recibió una de esas cartas. Era la variante de la herencia. En ella, el mensaje asegura que un tío olvidado que hizo

fortuna en las Américas ha muerto sin dejar descendencia directa y el incauto es el pariente más cercano. Como el señor daba la casualidad de que de verdad tenía un pariente en Venezuela, creyó la historia y lo puso en manos de un conocido bufete de abogados, los cuales aceptaron gestionar todo a cambio de un jugoso porcentaje. Las cantidades que iban reclamando los estafadores las adelantaron los letrados. Cuando se dieron cuenta, ya habían perdido mucho dinero y, lo que es peor, la confianza de su cliente.

La versión de la Lotería Nacional, como decíamos antes, está formada a menudo por grupos que operan desde España. Se estima que envían seis millones de correos electrónicos al año, en los que ofrecen premios de alrededor de seiscientos mil euros por los que había que pagar entre medio y dos puntos porcentuales en concepto de impuestos. En 2007, el Cuerpo Nacional de Policía realizó una importante operación en la que se detuvo a ochenta y siete personas, todas ellas de nacionalidad nigeriana, veintiocho de las cuales ingresaron en prisión preventiva, por realizar este engaño. Se calcula que habían obtenido un beneficio de más de ciento setenta millones de euros. Tan solo se habían presentado mil doscientas denuncias, con una media de dieciocho mil euros por afectado. Es decir, que a pesar de su obviedad, el negocio funciona bien. Solo con un uno por mil de éxito en sus envíos ya estarán consiguiendo engañar a seis mil inocentes.

Dentro de esta categoría, que no necesita especiales conocimientos informáticos, podemos incorporar todas las falsas ventas, en especial de vehículos (el conocido como «timo del coche inglés»), muy habituales en las páginas de compraventa entre particulares. En algunos momentos ha llegado a haber más anuncios falsos que verdaderos, a pesar de los esfuerzos de los administradores por detectarlos, eliminarlos y, si procede, denunciarlos. La mecánica es sencilla. Los rastreadores de la red descargan fotos de vehículos en óptimas condiciones de las propias páginas y, cuando estos son vendidos, vuelven a colocarlos como si fueran suyos, con unos precios mucho más baratos de lo que procedería incluso para un comerciante desesperado. Los incautos que preguntan recibirán un mensaje estándar, que suele estar en un español más decente que en otras especialidades, donde cuentan que es un automóvil matriculado en nuestro país por un británico que ha vuelto a casa. Allí no es capaz de venderlo al estar el volante al otro lado, de ahí la maravillosa oferta. Por supuesto, no pueden ofrecer más imágenes que las ya puestas y las respuestas a preguntas concretas suelen ser vagas en el mejor de los casos. Si el comprador cae en la trampa, algunos grupos incluso tienen un sistema de seguimiento en que se puede comprobar cuándo lo embarcan y en qué punto oceánico está el carguero que lo trae. Así pueden retrasar semanas o hasta meses la denuncia, tiempo suficiente para borrar todo rastro.

En diciembre de 2015 la Unidad de Investigación Tecnológica de la Policía Nacional desarticuló una red formada por españoles que operaban con la enésima variante de este delito. En este caso eran diez individuos que anunciaban falsos

apartamentos para vacaciones en Gandía, Fuengirola o Benidorm. Para ello, como en el caso anterior, recurrían a fotos de verdaderos alquileres que extraían de Internet. A la víctima le solicitaban un giro de entre doscientos cincuenta y trescientos cincuenta euros en concepto de anticipo, que debía remitir por giro postal. Para recogerlos tenían contratado a un numeroso grupo de toxicómanos del madrileño barrio de San Blas. De esta forma, creían quedar a salvo de la acción policial, a la que tan solo exponían a los cabezas de turco. Lo que no sabían era que los agentes los habían detectado en febrero y llevaban monitorizando desde entonces sus movimientos, cada teléfono móvil que compraban y cada cuenta de correo que creaban para sus engaños.

JUGANDO CON EL AMOR Y EL SEXO

Los estafadores no tienen reparos en utilizar cualquier recurso para desplumar a sus víctimas, bien sea la avaricia… o el corazón de los más solitarios. Es bien conocida la existencia de unos sitios de Internet que ofrecen «novias rusas por catálogo». Alrededor de estas agencias matrimoniales legales se ha creado una serie de mitos sobre la belleza y accesibilidad de las mujeres eslavas que, desde al menos 2007, han derivado en el conocido como *timo de la novia rusa*, que es una variante más de las cartas nigerianas que merece un apartado especial. Según el Departamento de Estado de los Estados Unidos, solo entre ese año y el siguiente estafaron más de ocho mil millones de dólares en todo el mundo. La diferencia con las anteriores estafas está en el gancho. No buscan el bolsillo, sino los sentimientos. Usan fotografías legítimas que encuentran en diferentes sitios de Internet, todas de muchachas guapas y solteras. Sirviéndose de ellas, nos cuentan que han tenido la suerte de encontrarnos «en Internet» y les parecemos de lo más interesante. Por supuesto, en posteriores correos se enamoran de nosotros con locura y su único deseo es venir a vernos. Ahí está la pega. Necesitan que les paguemos el visado, el soborno a los policías de aduanas, el billete y lo que se tercie hasta que la víctima desista. La ventaja de este tipo de estafa es que quien la sufre está poco dispuesto a denunciar ante el oprobio de reconocer lo que le ha pasado ante cualquier otra persona, policía incluida. Suelen ser personas sin muchas habilidades sociales para los que poner la denuncia formal representa una nueva humillación.

En un paso más sofisticado, algunas mafias, en especial del norte de África, decidieron ampliar la escala y, en vez de buscar los sentimientos, van por las gónadas. Así nació la *sextorsión* organizada. El chantaje por motivos sexuales vergonzantes es tan antiguo como Internet, si bien lo habitual es que quien lo comete lo haga por motivos lúbricos, como vimos en el capítulo segundo; es decir, la violencia se dirige a obtener más imágenes sexuales una vez conseguidas las primeras o a mantener relaciones íntimas con el agraviado. La novedad la ha constituido construir verdaderas redes de *agentes contratados* que funcionan a comisión.

La estafa típica comienza con un perfil en las redes sociales, a menudo en Facebook, aunque sin descartar otras más minoritarias y orientadas al ligoteo, como Badoo o Tinder. El extorsionador se ha creado un perfil seductor —en ocasiones es incluso su propia imagen con datos de identidad falsos— y agrega o espera ser agregado por corazones solitarios o con una vida sexual insatisfactoria. Siempre son hermosos, tanto hombres como mujeres, y parece fuera de lugar ese comportamiento que no deberían necesitar para obtener pareja, dadas sus cualidades. Al contrario que en la estafa de la novia rusa, aquí el tratamiento personal es más importante. Los mejores pueden pasarse días o hasta semanas con un mismo individuo que mantenga conversaciones privadas con ellos. Poco a poco, dependiendo de la habilidad de cada cual, las conducirán hacia una temática sexual, buscando la exhibición de aquel a quien hacen sentir en una cómoda ciberrelación de pareja. No dudarán en mostrarse ellos. En ocasiones son sus cuerpos de verdad. Las más, son vídeos que, mediante programas como Fake Webcam, hacen pasar por verdaderos. Si consiguen su propósito, les mostrarán que han capturado su emisión de webcam y que deben pagar una cantidad que oscila entre los quinientos y quince mil euros para no revelarla al resto de sus contactos de Facebook. Como el proceso de ganar la confianza ha durado tiempo, saben suficientes cosas del objetivo para conocer los puntos débiles. Muchas veces son personas casadas o jóvenes que viven con sus padres y ellos serán los primeros que reciban los vídeos. Hacerlos llegar al entorno laboral o escolar es el siguiente paso. La mayoría paga por pánico —a través de los medios no rastreables que hemos visto— y no denuncian por vergüenza, con lo que el alcance total es difícil de calcular, pero los beneficios de estas mafias se estiman en decenas de millones de euros anuales. Los cabecillas de las organizaciones suelen estar en países del norte de África, mientras que sus *agentes* están por todo el mundo. En el caso de aquellos que muestran su verdadero rostro, son más habituales en países del Este de Europa y, cada vez más, de Asia y el Pacífico, con una especial incidencia en Filipinas. Una variante de la estafa incluye mostrar imágenes de lo que parece ser un menor de edad y, en ese momento, remitir una carta a la víctima en la que se le comunica que está siendo investigado por corrupción de menores y que debe pagar de inmediato una multa para librarse de los cargos. Es obvio que ninguna policía del mundo remite una misiva al autor de delitos tan graves.

En verano del año 2013, Daniel Perry, un chaval británico de diecisiete años, saltó desde un puente cerca de Edimburgo al no poder soportar más el acoso que estaba sufriendo tras haber caído en las garras de una de estas organizaciones. Interpol coordinó una operación para acabar con esa trama que concluyó en mayo del año siguiente en Filipinas, con la detención de cincuenta y ocho personas, incluidas las tres implicadas de forma directa en ese suicidio inducido, y la incautación de doscientos cincuenta elementos informáticos. Solo uno de los jefes había conseguido dos millones de dólares de beneficio en poco tiempo. Sus víctimas se contaban por centenares en el Reino Unido, Hong Kong, Malasia, Singapur, Estados Unidos,

Australia y la propia Filipinas. Funcionaban como una empresa regular, con una *oficina* en un barrio marginal de Manila en la que multitud de mujeres trabajaban por turnos, e incluso había pizarras con los logros y estadísticas de cada una de ellas.

Este timo afecta tanto a hombres como a mujeres. Si bien estas son más reacias a la hora de desvelar sus intimidades, también sufren más las posibles consecuencias, por motivos sobre todo de educación.

En realidad es fácil salir de esta trampa si no se ha sabido detectar a tiempo. Hay que cortar toda relación con el chantajista y ponerlo de inmediato en conocimiento de la policía.

CUANDO LA TECNOLOGÍA ES LA BASE

Las estafas que hemos visto hasta ahora son bastante básicas. No hacen falta unos conocimientos de informática exhaustivos, sino tan solo una soltura suficiente a la hora de manejar Internet y los ordenadores. Están basadas en el simple engaño. Cuando se cuenta con un equipo de programadores en la estructura criminal, se puede ir un paso más allá y conseguir un beneficio mucho más alto accediendo, sin intermediarios, a las cuentas bancarias de los incautos.

La primera de las modalidades, más sencilla, se conoce en argot como *phishing*, del inglés *fishing*, pescar. Es una analogía en la que las víctimas actúan como peces y el delincuente como un arrastrero, lanzando redes al por mayor —recordemos que el triunfo de estos delitos se basa en llegar a mucha gente, dado que la inmensa mayoría no pica—. Es un término acuñado a mediados de los noventa para el robo de correos electrónicos, como veremos en el capítulo octavo de este libro, cuando hablemos de técnicas de *hacking*. En él se establecieron los patrones básicos que hoy se siguen utilizando.

La red desarrolla dos herramientas diferentes. La primera, un correo electrónico que suplanta, de la manera más verosímil posible, a un banco concreto. Para ello usarán sus logotipos, tipos de letra y hasta advertencias legales al pie, con lo que se encuentran contradicciones tales como que se está intentando convencer de hacer lo mismo que se prohíbe en los párrafos finales del mismo mensaje. Las muchas variantes —tantas como da la creatividad humana— siempre acaban en una misma condición, que por algún motivo el banco necesita que el cliente introduzca todos los códigos que le han sido proporcionados para operar con la banca *online*.

Para recopilar la información es necesario el segundo de los trabajos de la organización, una página web de nuevo con los logotipos de la entidad y un formulario para que la víctima teclee hasta el último de los dígitos de su tarjeta de coordenadas. Una vez introducidos, se redirige al cliente a la página legítima del banco para limitar las sospechas. Este señuelo lo colocan dentro de sitios web legítimos con poca seguridad o en servidores comprados al efecto en países con un

control laxo sobre las actividades ilegales. Un usuario medio de Internet, mirando la dirección en el navegador podrá detectar en un instante el engaño, dado que suelen ser del tipo *http://servidorFalso.bizz/laCaixa.es* o *bbva.es.engaño.xxx* y, en general, son eliminadas por las autoridades competentes en poco tiempo, a veces horas, casi siempre un par de días. El objetivo de la estafa es quien no sabe lo mínimo imprescindible, ese vulnerable cuatro por ciento, como ancianos o despistados tecnológicos. Dado el volumen de mensajes enviados, es más que suficiente para obtener un buen rédito. Las entidades bancarias y la policía avisan a menudo de que el banco jamás va a pedir los datos que ya posee, menos aún en un correo de procedencia incierta. El objetivo es reducir lo más posible el número de incautos. Por las leyes de la sociología, siempre habrá un pequeño porcentaje. El objetivo es que sean los menos posibles.

Una vez que tienen acceso a las finanzas del objetivo, el siguiente paso es vaciarla de efectivo. Las mafias no reparan en si están atacando a un magnate o a un pensionista. Extraerán, si pueden, hasta el último céntimo. No lo van a remitir de forma directa a una cuenta bancaria propia. Aquí entran en juego los *muleros* de los que hablábamos al principio. La trama les va a ingresar en sus propias cuentas bancarias el dinero de los desplumados a través de transferencias electrónicas desde la cuenta corriente de la que se han apoderado. Su misión es extraerlo y canalizarlo por empresas de envío de remesas, donde se les pierde la pista y acaban en manos de la organización criminal.

Los delincuentes de países de la órbita rusa son los maestros de esta especialidad. La mitad de toda la actividad de *phising* cometida en el mundo en el año 2006 utilizaba los servidores de una empresa llamada Russian Bussiness Network (Red de Negocios Rusos) ubicada en la ciudad de San Petersburgo. Tan solo uno de esas bandas mafiosas, conocida como Grupo Roca, que robó ciento cincuenta millones de dólares, ubicó en esa compañía las webs destinadas a crear el engaño. Entre 2012 y 2015 en todo el mundo, en especial sus países de origen (Rusia, Ucrania, Bielorrusia, etc.), aunque también en la Unión Europea y Estados Unidos, se ha detenido al menos a ciento sesenta miembros de organizaciones medianas y grandes que habían obtenido un beneficio ilícito de al menos setecientos noventa millones de dólares.

El *phishing* tradicional está dedicado de forma muy especializada al robo de servicios de banca *online*, donde ha probado ser tan lucrativo como hemos visto. Sin embargo no es la única modalidad. Ante las continuas campañas y avisos contra estas trampas y el hecho objetivo de que el *mercado* está muy saturado, algunos grupos están volcando sus esfuerzos hacia otras versiones menos lucrativas pero también menos protegidas. Algunas se dirigen a plataformas de venta *online* como eBay. El objetivo en este caso es hacerse con el control de cuentas que tengan mucha reputación —de forma parecida a lo que hemos explicado en el capítulo anterior al hablar de los vendedores de Silk Road, pero en versión legal— y suplantarlos para ofrecer productos ficticios. Los compradores, confiados en la buena valoración,

pagan sin dudar. El delincuente convencerá a su víctima de que realice el pago por medios no rastreables y de esta manera se saltan la necesidad de una *mula*. Una cuenta usurpada de esta naturaleza tiene una vida muy breve. Por un lado, enseguida empezará a recibir puntuaciones negativas y, por otro, los servicios antifraude de las plataformas suelen detectar el cambio de hábitos de venta de forma muy rápida.

Otro ataque habitual es a usuarios de plataformas de pago *online*, como la celebérrima PayPal. Uno de los objetivos más simples en este caso es realizar compras a cargo del legítimo titular y luego recogerlas por miembros de la banda en diferentes lugares. Después, esos bienes son a su vez vendidos a muy bajo coste. De ahí proviene el beneficio.

En los últimos años se ha detectado también una vuelta al origen de la palabra y lo que intentan los criminales es conseguir acceso a correos electrónicos. En el pasado los *emails* recibidos se guardaban en los ordenadores, pero en la actualidad predomina el uso de *webmails*, como Gmail o Hotmail, donde lo más habitual es que se queden almacenados los correos en la nube. Tendemos a guardar datos muy importantes ahí, como registros en sitios web, muchos de ellos, comercios. De esta manera, si alguien tiene acceso a nuestro correo, podría comprar en nuestro nombre y remitírselo a donde más le interese, además de conocer muchos datos íntimos que pueden servir para una variante de las cartas nigerianas, la estafa del ciudadano en apuros. En esa versión, también de mafias africanas en la mayor parte de los casos, quien controla la cuenta de *email* asegura que su contacto está perdido en una situación muy apurada en algún lugar del continente negro y solicita a todos los miembros de la lista de contactos que le envíen un giro postal o transferencia de Western Union, que un miembro de bajo nivel de la organización recogerá en el destino. Muchas veces, el verdadero titular ni siquiera es consciente de estos hechos, dado que la trama intentará pasar lo más desapercibida posible, borrando los mensajes enviados y dejándolo todo como lo encontraron. Aunque el engaño sea fácil de desmontar —valdría una simple llamada telefónica— todos los años caen miles de personas.

En julio de 2015, la Policía Nacional, en colaboración con sus colegas de Italia, Bélgica y Polonia, participó en una operación en la que se detuvo a cuarenta y nueve personas y se intervinieron nueve mil euros y mucho material informático y telefónico con los pormenores del funcionamiento de la red, formada por nigerianos, cameruneses y españoles. Su objetivo no eran los ciudadanos corrientes, sino los correos de grandes empresas, de los que se apropiaban con las técnicas que hemos explicado. Una vez que lograban acceder —dado que el usuario, engañado, les había dado la contraseña—, espiaban con sumo cuidado los mensajes entrantes y salientes hasta que detectaban los que les interesaba, aquellos en que una empresa iba a pagar a otra. Lo modificaban, cambiando los números legítimos por el de una que tenían bajo su control. Así pues, cuando el pagador hacía la transferencia, no llegaba al deudor, sino que era desviada a cuentas de los *muleros* a sueldo de la organización, que lo

extraían y lo enviaban fuera de la Unión a través de los medios habituales.

EL DELICADO LÍMITE ENTRE LA ESTAFA Y EL ATAQUE INFORMÁTICO

El *phishing* requiere de la cooperación de la víctima para conseguir su objetivo. Los verdaderos *maestros del crimen* tratarán de evitar la voluntad del *pardillo* e ir un paso más allá, que el responsable del engaño sea el ordenador y no la inocencia.

Como vimos en el capítulo uno, Internet funciona a través de direcciones IP. Que cada una esté asignada a un nombre (como *esferalibros.com*, cuya IP es 84.246.209.30) es algo que se gestiona a través de los llamados Servidores de Nombres de Dominio —DNS por sus siglas en inglés— y que sirve para hacer la vida más fácil al usuario, al que recordar números al azar suele resultarle complicado. Nuestros ordenadores guardan en sus tripas un archivo donde están las correspondencias para las páginas que consultamos de forma habitual. De esa forma, al evitar consultas, se gana velocidad de navegación.

¿Qué pasaría si alguien pudiera modificar el servidor o nuestro ordenador y poner, en lugar de las direcciones de los bancos, la suya propia? Esto requiere una mayor sofisticación. No solo hay que crear y alojar las páginas falsas en sitios, sino realizar ataques informáticos a los servidores o preparar un virus que infecte los ordenadores de los usuarios y les cambie ese archivo. Esta modalidad se llama *pharming*, del inglés *farming*, labranza, por un juego de palabras con la *pesca* del *phishing*.

El primer tipo de acción es muy difícil. Los servidores DNS son máquinas con una gran seguridad y cualquier modificación se detectaría en un breve periodo de tiempo. Sin embargo, los ordenadores particulares son mucho, mucho más vulnerables. Sorprende encontrar, todavía hoy, una ingente cantidad de personas que no tienen ningún antivirus instalado. Como ya dijimos, la pregunta no es si sufrirá una intrusión, sino cuántas está sufriendo ya.

El esquema de esta estafa se inicia de forma similar al de *phishing*. Siempre hay que llegar al incauto, de una u otra manera. En este caso el objetivo es colocarle el *bichito* que han creado —o comprado— los mafiosos. Aunque se puede intentar ubicar en páginas web aprovechando vulnerabilidades, eso requiere un trabajo extra para el que no todos están capacitados. El método más habitual vuelve a ser el correo electrónico con *gancho*. En este caso basta con que abra un archivo infectado. Intentan que el mensaje cause engaño suficiente. Son habituales mensajes como «¿Esta foto que me han pasado es tuya?» o «Le adjunto la factura por valor de 200 dólares». Por supuesto, no es una foto —no son *ejecutables*, es decir, no tienen un programa dentro, y nunca puede estar infectado— ni una factura, sino el temido virus que modifica las DNS del ordenador. La inmensa mayoría de antivirus identifica esas amenazas, pero claro, es necesario tenerlo.

Una vez que ha efectuado su *magia* y cambiado el pequeño fichero de Windows que almacena a qué IP corresponde cada página web, solo tienen que esperar. Cuando el usuario teclee en su navegador la dirección de su banco, la página a la que accederá será la fraudulenta. En todos los sentidos parecería la correcta, por lo que el incauto, confiado, está mucho más dispuesto a introducir las claves. Una vez hecho, actúa como en la tipología anterior, redirige a la web legítima y los ladrones ya pueden vaciar los fondos del ciudadano.

Cuando se detectó la vulnerabilidad, Microsoft se apresuró a corregirla, protegiendo el archivo —llamado *host*— de forma que en cualquier sistema operativo actualizado el ataque tiene muy pocas posibilidades de tener éxito. En otros entornos, como los basados en Unix, la protección es menor, aunque debido a la escasez de víctimas potenciales, apenas tienen amenazas. Cuesta lo mismo generar un virus para Windows que para Unix, pero los primeros son más del noventa por ciento del mercado.

La amenaza del *pharming* prevalece. Hay una manera de sufrir el ataque de forma que ningún antivirus puede protegernos. Además de en el ordenador hay otro lugar que almacena una lista de correspondencias entre IP y webs: el *router*. En principio, para infectarlo haría falta meter un *malware* que, de nuevo, los antivirus detectarían, puesto que deberían pasar por el PC. Uno de esos encontró, en enero de 2008, la compañía de seguridad informática Symantec. Los delincuentes enviaron de forma masiva correos electrónicos, como ya hemos visto en casos anteriores, que simulaban ser una postal electrónica de la empresa *gusanito.com*, una web legítima dedicada a remitir ese tipo de animaciones en las que se puede esconder un virus con facilidad. Al ejecutarlo, se modificaba la configuración del *router*, de manera que reemplazaba la página web de un banco mexicano cuyo nombre no trascendió. Todos los que accediesen desde ese instante a la red que gestionaba ese dispositivo, eran conducidos a la página fraudulenta.

Con la extensión de las redes inalámbricas —casi cada hogar tiene una en España — aumenta la posibilidad de esos ataques sin necesidad de programar complicados *bichitos*. Por desidia o desconocimiento, muchos usuarios no cambian la configuración por defecto de sus *routers*. Desconocen que las contraseñas son estándar. Es decir, que por cada modelo hay un número escaso y concreto de cifras y números que introducir. Una vez que el intruso ha accedido a la red —hay programas gratuitos que lo hacen y se pueden descargar para cualquier teléfono móvil— puede modificar lo que le interese. Incluido, por supuesto, el archivo de DNS del *router*, con el que pueden jugar como más les interese. Como el ordenador no ha sido afectado, no es fácil darse cuenta de lo que está pasando. Hacerle esa operación —para la que hay que estar relativamente cerca— a un usuario doméstico puede no salir a cuenta, pero la cosa cambia con *WiFis* públicas. Las más fáciles de atacar son las de comercios pequeños y restaurantes, que a menudo no incorporan más seguridad que la de un domicilio. Las de centros comerciales o aeropuertos son un objetivo mucho

más difícil a la par que tentador. Si una organización consigue alterar ese servicio, las víctimas potenciales pueden ser decenas de miles, con lo que aumenta la posibilidad de que alguna sea cliente del banco cuya web ha sido suplantada y caiga en la trampa. Ese es uno de los motivos por el que se desaconseja utilizar la banca *online* desde lugares de acceso públicos.

Algunas tramas criminales son hasta más complejas. Consiguen *inocular* virus en los ordenadores o teléfonos de las víctimas y los bloquean a cambio de un rescate. Si bien también se puede considerar una estafa, vamos a tratarlo más adelante, en el capítulo dedicado a los ataques informáticos, dado que, aunque el propósito final es el económico, encaja más con aquel que con la simple estafa.

OBJETIVO: LA TARJETA DE CRÉDITO

Una de las actividades más comunes entre las mafias es el conocido como *carding* o sea, los diferentes procedimientos para apropiarse de números de tarjeta válidos y obtener con ellos ganancias, bien en efectivo, bien en especie. En el capítulo anterior vimos cómo un ciudadano español había conseguido introducirse en el servidor central de un banco, desde el que obtenía numeración válida que luego vendía en el mercado negro. Es una de las muchas formas que adopta esta especialidad.

Una de las maneras más habituales de controlar una tarjeta de crédito ajena es montar un negocio virtual «falso», en el que se ofrecen productos a unos precios muy inferiores a los del mercado —en ocasiones, hasta un noventa por ciento más barato —. Sus formularios de compra no suelen ir bajo protocolos seguros —*https*, que encriptan los datos, en vez de *http*—. Estas páginas suelen ser de corta duración y se puede encontrar muchos comentarios negativos sobre ellas en cuanto se hace una búsqueda sencilla.

También se realizan ataques a páginas web legales poco protegidas. Los comercios en línea legítimos no cobran por sí mismos, sino que realizan una *llamada* a una web de cobros seguros que, tras realizar la compra, nos devuelve al comercio electrónico. Si este no está bien protegido o ante delincuentes con una especial habilidad, podrían alterar la programación del sitio y sustituir la plataforma de pagos por su propio *clon* que, por supuesto, enviaría los datos de las tarjetas a su sistema antes de redirigir a la verdadera web de cobros.

Hay muchos foros en español, incluso en la Internet abierta, sobre cómo hacer *carding*, a qué problemas se van a enfrentar y cómo solucionarlos. En el colmo de la desfachatez, es normal leer consejos para evitar, a su vez, ser timados, ya que se quejan de que hay mucho estafador que quiere hacer negocio con los aprendices de ladrón.

La forma más tradicional —aunque también arriesgada— de obtener números de tarjeta de crédito es el conocido como *skimming*, esto es, la copia de una tarjeta de

manera física. Para ello hay dos formas principales, o bien tienen empleados que forman parte de la organización en comercios —en España, restaurantes y gasolineras, sobre todo; en otros lugares del mundo puede ser casi cualquier lugar— o bien modifican cajeros electrónicos. En alguna ocasión la alteración ha sido tan sutil —y complicada— como colocar un chip en las «tripas» del cajero, en el cable que lleva los datos recién introducidos —de tarjeta y pin asociado—, que lo mandaba vía radio a una ubicación desconocida, aunque, dado el alcance, cercana. La mayor parte de las ocasiones no son tan sofisticados. Suelen instalar un lector de tarjetas sobre el legítimo, de manera que primero la copia y luego la introduce en el correcto. Para obtener el PIN colocan microcámaras sobre el teclado para comprobar las pulsaciones de todo el que lo usa. Algunas bandas utilizan pulsadores de goma instalados sobre el de verdad, con lo que la acción de tapar con la mano lo que se teclea resulta inútil en esos casos. Han llegado a recrear frontales de cajero completos, hasta con los logotipos del banco, que han adherido al original y luego retirado, amparados en la quietud de la noche. Los bancos han aprendido mucho y la época dorada de esta técnica de robo ya ha pasado. Por un lado, sus servicios antifraude detectan con facilidad cuándo un cajero ha sido *comprometido* y bloquean todas las tarjetas afectadas. Por otro lado, las propias máquinas incorporan ahora una notable cantidad de elementos de seguridad para evitar estas acciones, hasta el punto de hacerlas casi imposibles. Es fácil hacerse con el material para realizar *skimming* en cualquier mercado negro de los vistos en el capítulo anterior. La capacidad para realizar el artefacto completo y colocarlo ya depende de las habilidades técnicas de cada cual, aunque los tutoriales son sencillos de encontrar.

En cualquier caso, una vez obtenidas las tarjetas, por uno u otro sistema, hay que darles salida. Las redes de diversos países se ponen en contacto entre sí para intercambiar números de tarjeta, de forma que las clonadas en Rumanía se usen en España y las españolas en Venezuela, por ejemplo. Estos viajes de las tarjetas se hacen para dificultar la acción policial, dado que la colaboración transfronteriza siempre es complicada en delitos económicos. En sitios como Alphabay, Nucleus o en la fenecida Silk Road es fácil encontrar tarjetas, cuentas de PayPal o de cualquier negocio electrónico por precios más que asequibles.

Los compradores, bien al por mayor o clientes finales, las utilizarán para obtener bienes o dinero, según sus capacidades y especialidad. En abril de 2015, la Policía Nacional detuvo en España a cincuenta y cuatro individuos que tenían montado un negocio muy sofisticado. Contrataban a personas sin recursos para que dieran de alta TPV en todos los bancos que pudieran, asociados a empresas fantasmas —cerradas o sin actividad—. Esos *prescindibles* entregaban los aparatos a miembros de pleno derecho de la red y ahí acababa toda su relación con la misma. Mientras tanto, personal de más alto nivel contactaba con los *clonadores*, que trabajaban en Estados Unidos, Colombia, República Dominicana y Venezuela. Estos se dedicaban a copiar cuantas tarjetas podían en sus lugares de origen, que enviaban a España. Aquí se

usaban los TPV adquiridos para realizar el máximo número posible de compras ficticias, que de inmediato transferían a diferentes cuentas bancarias. Ahí, de la forma habitual, los *muleros* las extraían y remitían. Los *buscadores* que se encargaban de encontrar a los que daban sus datos para adquirir TPV tenían una tupida red de intermediarios para evitar que aquellos, al menos inocentes en parte, supieran para quién trabajaban de verdad.

Otra banda similar fue desmantelada por la Policía Nacional a finales de diciembre de 2015. En este caso eran cinco personas que defraudaron cuarenta y cinco mil euros con las tarjetas que recibían de su cómplice, que las clonaba en la República Dominicana. Con ellas compraban en diversos comercios de Madrid joyas y telefonía móvil, que luego revendían de segunda mano. Otra forma de convertir en efectivo el dinero robado.

Como vemos, conseguir copias de tarjetas es relativamente fácil. Lo difícil es utilizarlas y que la policía no te atrape.

OTRAS ESTAFAS: ALLÍ DONDE HAYA DINERO

Internet está lleno de intentos de estafa. Correos para que compremos medicamentos, webs de productos a bajo precio o programas inexistentes. El objetivo es conseguir el dinero del primo lo antes posible. No hace falta siquiera ser un *genio del mal* para conseguirlo.

Algunas de las más corrientes en España consisten en recibir llamadas telefónicas que indican que hemos ganado un premio y que para reclamarlo debemos llamar a un teléfono de tarificación adicional.

Otra muy habitual consiste en que una web nos solicite el número de teléfono móvil para un presunto e inexistente sorteo. En realidad, nos suscriben a un servicio de SMS *premium* por el que nos cobran hasta treinta euros diarios por enviarnos publicidad.

Internet es bastante seguro en realidad. Solo hay que moverse con precaución a la hora de gastar dinero y, por supuesto, no creer fantasías de ligues imposibles o chollos extraordinarios. Con eso y un poquito de información podemos estar a salvo de casi todo.

7

EL DINERO QUE EXISTE Y NO EXISTE A LA VEZ

La habitación está llena de humo de tabaco. El centro está ocupado por una fila de monitores antiguos, de los cúbicos, que ocupan gran espacio. Se impone el zumbido de los ventiladores de decenas de ordenadores que se afanan por refrigerarlos en un ambiente cálido y saturado. En las pantallas se muestran los últimos juegos online, aquellos que tienen más jugadores al mismo tiempo. En una esquina, una mesa en la que un chico de unos veinte años come con palillos un cuenco de arroz. A su lado, otro se ha levantado las gafas y se frota los ojos, cansados de permanecer doce horas seguidas fijos en sus partidas. En la habitación de al lado, unas literas y colchonetas tiradas por el suelo para aquellos que han cumplido su jornada y necesitan descansar un poco. Todo el lugar está en penumbra. Así, la luz natural no les distrae de sus tareas. Estamos en la próspera Shanghai, en China, aunque en ese peculiar piso patera no se vea la abundancia por ningún sitio. Eso sí, cada uno de los ochenta trabajadores que se turna en los cuarenta equipos conectados a Internet cobra más que el sueldo medio de la ciudad, uno de los más altos del país. Su patrón paga los correspondientes impuestos por su actividad, legal, aunque sabe que no superaría una muy poco probable inspección de las autoridades. En su cultura nadie tiene miedo al trabajo duro. Doce o catorce horas son una bicoca.

La labor de los jóvenes, de ambos sexos, es repetitiva. No están disfrutando del juego, al menos no como la mayoría de los que lo hacen. Algunos están generando productos de bajo coste como armas, alimentos u oro virtual. Otros están peleando reiteradamente contra el mismo enemigo —que reaparece al poco tiempo tras ser eliminado— para hacer subir niveles al personaje que manejan. Cada vez que consiguen llegar al máximo, le entregan los datos al jefe y vuelven a empezar desde el principio. Cuando tienen un poco de tiempo o quieren cambiar de actividad, se dedican a crear personajes nuevos y matarlos para poner sus cuerpos en forma de letras que pongan un mensaje, para indicar dónde pueden encontrarlos y contratarlos.

El jefe consulta una serie de tablas disponibles en Internet con sus fluctuaciones diarias, como cualquier mercado bursátil. Gracias a ello sabe cuántos dólares puede pedir por cada material que sus chicos generan para él. En Chicago, en Madrid, en Marsella, en Turín… sus clientes están por todas partes. Los gamers cada vez son más adultos y no tienen tiempo para ir progresando a lo largo del juego; lo necesitan para trabajar y atender a sus familias. Prefieren comenzar desde arriba y para ello no les importa pagar con dinero real a cambio de bienes virtuales que, de hecho, solo existen dentro de un muy determinado mundo de ficción que un día desaparecerá

igual que fue creado. Ahí entra él. Bueno, él y sus miles de competidores que hacen lo mismo. La legislación china permite comprar productos intangibles con dinero real, pero no a la inversa —uno no puede comprar un coche y pagarlo con el oro que posee su personaje del League of Legends—. Así, el negocio progresa. Los occidentales —y algunos millonarios compatriotas— tienen lo que desean y él se enriquece mientras paga salarios generosos a sus trabajadores. Es una buena época para vivir.

LAS LEYES DE LA ECONOMÍA SON UNIVERSALES

La industria del videojuego se ha sabido adaptar a los nuevos tiempos mejor que otras más tradicionales, como la música o el cine. Está ligada como ninguna otra a la tecnología disponible en cada momento, por lo que es más flexible y adaptativa que otras que llevan más de un siglo entre nosotros. Mueve una cantidad de dinero ingente. Ese mercado está valorado en más de cien mil millones de euros y un solo juego, como *Call Of Duty: Black Ops* alcanzó, en tan solo los cinco primeros días tras su lanzamiento, unas ventas de seiscientos millones de euros.

La copia ilegal les hizo perder muchísimo dinero a principios de siglo, hasta que fueron conscientes de que luchar a base de restricciones contra la piratería es imposible o, al menos, más costoso que buscar caminos alternativos. Aparte de consolas cada vez más difíciles de modificar para que acepten productos descargados de una web ilegal o de unos precios tan competitivos que hace ridículo no comprarlos, el mejor camino ha consistido en aprovechar los propios recursos que da Internet. Ya no es la época en que cada persona juega aislada en su casa; ahora se puede estar interconectado con miles de otros jugadores. Si se está cada día en las redes sociales, ¿por qué no se puede hacer lo mismo en otros ámbitos?

El problema fue el ancho de banda. Al contrario que la mayor parte de las actividades que se hacen en línea, los juegos necesitan intercambiar a gran velocidad una ingente cantidad de datos. La línea telefónica tradicional sobre la que trabajaban los módems de fin de siglo carecía de la capacidad para ello. Nacieron los cibercentros, donde las partidas se jugaban en su interior, a menudo dentro de la red local del negocio o utilizando la conexión rápida de la que ellos sí disponían, pero que resultaba prohibitiva a un particular. El *mundo* duraba el tiempo del juego. Al acabar, todo volvía a sus posiciones de salida.

Algunos acudían a jugar al primer MMORPG —Juego de Rol Multijugador Masivo En Línea, por sus siglas en inglés— que se popularizó, el *Ultima Online*. Al contrario que en los anteriores, el universo era persistente. Cuando el suscriptor se desconectaba, todo seguía existiendo, otros jugadores interactuando y las acciones propias y de otros tenían una consecuencia perdurable para el momento en que se decidiera retomar la partida. Mostraba la mayor parte de las características de los

programas de ese estilo, una serie de misiones que cumplir, cada vez más complicadas a medida que el personaje avanzaba, un sistema de recompensa en forma de puntos de experiencia que servían para subir habilidades y una economía compleja, diseñada desde un principio para ser omnicomprensiva y equilibrada. Se ganaba *oro* virtual matando enemigos, encontrando tesoros o manufacturando objetos que luego eran vendidos a pequeños programas llamados *personajes no jugadores* que, por ejemplo, eran los dueños de una tienda. Para subir algunas habilidades, los usuarios tenían que realizar la tarea monótona de crear un determinado tipo de artesanía decenas o centenares de veces. Llegó a haber tantos productos de un mismo modelo que, de acuerdo con las leyes de la oferta y la demanda, su valor cayó casi a cero, por lo que no se podían vender. Los jugadores perdían mucho tiempo en algo que no les reportaba beneficio económico. Esto causó quejas a los diseñadores, que modificaron los patrones de manera que las tiendas siempre compraban lo que se les vendía por un precio mayor del que dictaba el mercado. Esto representó un gran aumento en el *oro* disponible —es decir, el juego cada vez tenía más efectivo en circulación—. Como consecuencia, la inflación se disparó. ¿Cuándo ocurre ese fenómeno? Igual que en la vida real. Cuanto más dinero hay disponible, más se está dispuesto a pagar por un mismo artículo y, por tanto, más caro es todo. De esta forma, los jugadores novatos se veían imposibilitados de adquirir bienes necesarios con el capital disponible y lo que se obtenía de matar monstruos o de tesoros no era suficiente, por lo que se debían dedicar a labores de manufactura, un *trabajo* aburrido para el que no apetece pagar la suscripción mensual que da derecho a acceder a los servidores donde se aloja ese mundo virtual. Si se tiene un cierto nivel económico, quizá mereciera la pena pagar a alguien por hacer ese trabajo.

En 2003, Linden Lab lanzó *Second Life*, segunda vida, un juego diferente a todo lo que había en ese momento. Es gratuito —al menos, para lo más básico— y se lleva a cabo en un universo persistente —o *metaverso*— alojado en sus servidores. Con independencia de quién esté conectado en cada momento, las acciones realizadas en él continúan y tienen un efecto. Este entretenimiento, al contrario que la inmensa mayoría, no tiene una misión concreta que cumplir. No hay dragones ni princesas, no hay tesoros ni aventuras mágicas. Su único propósito es permitir al usuario vivir lo que en su día a día no puede. Conseguir ser el artista alternativo que siempre deseó, cambiar de sexo o dedicarse al gamberrismo. Lo primero que se ha de hacer es crear un personaje o avatar que va a representarnos. Tiene una serie de opciones básicas, desde cada rasgo de su físico a la ropa que va a llevar, dentro de unos estándares. A partir de ahí, aparece en una calle del mundo virtual que, en gran medida, está construido por otros usuarios. Eso sí, para conseguir una casa, ropa más elegante o facultades extra —como volar— hace falta pagar. Para ello existe una moneda desarrollada por la empresa, el dólar Linden, que tiene un cambio variable que suele rondar los doscientos cincuenta por cada uno estadounidense, con una pequeña diferencia a favor de la empresa —es más barato venderlos que comprarlos—. Esta

moneda puede ser intercambiada o donada entre personajes, de forma que existe una transacción de dinero real (o, al menos, convertible).

Dejando a un lado las copias de tiendas físicas que tienen presencia en *Second Life* para vender productos que se envían a casa de quien maneja el muñequito, existe una verdadera economía compleja basada en el comercio de bienes y servicios de una forma a veces aterradoramente parecida a la realidad. Los personajes pueden tener trabajos *reales* por los que reciben un pago en dólares Linden. El más sencillo de ellos consiste, tan solo, en *estar* en ciertos sitios, por lo general, centros comerciales virtuales. Los jugadores tienden a acudir a los sitios en los que hay más avatares y no saben si la presencia de los otros es pagada o casual. Así, al acercarse a ver lo que ocurre, es más fácil que compren en las tiendas. También pueden contratar a un avatar como modelo, por ejemplo. Para ello debe tener unas características determinadas: hay que haber invertido en hacerlo más real que los más básicos, bien programando, bien comprando esas mejoras.

Los productos a la venta son prendas, texturas, movimientos más naturales que los andares robóticos que se obtienen de salida y hasta casas en las que hacer que viva nuestro sosias informático. Todo ello está escrito por particulares con conocimientos de programación o de diseño gráfico. Por supuesto, hay revendedores de productos que compran un original y lo copian para venderlo por una fracción de su valor. A veces se hace de manera legal y otras es algo muy cercano a la piratería de productos de marca. Hay gente que consigue mucho dinero con sus negocios y otros que obtienen algunas monedillas para subsistir. La empresa matriz apoya con decisión todo ese comercio legítimo con propiedad industrial e intelectual, ya que su principal fuente de ingresos es el cambio entre la moneda física y la electrónica.

Es tal la importancia de esta economía que el Departamento del Tesoro de Estados Unidos ha declarado al dólar Linden *moneda virtual centralizada convertible*. Una moneda virtual es aquella que se puede cambiar por dinero real o bien que se puede utilizar para comprar bienes y servicios. Que sea centralizada significa que hay una organización concreta que respalda su valor y controla su emisión —con lo que puede tener bajo control la inflación o deflación—. El emisor tiene una serie de obligaciones ineludibles, como son un sistema confiable antiblanqueo de dinero, para evitar que sirva para lavar bienes de procedencia ilegal y una emisión de informes periódicos sobre su actividad. Esto es demasiado rígido para permitir que los delincuentes lo utilicen con profusión.

Mientras Linden Labs se lanza sin reservas a facilitar el comercio en su juego estrella, otras compañías lo combaten con energía, dado que les traen más perjuicios que beneficios. Sus monedas no son cambiables por dinero real, aunque sí entre personajes.

Los juegos masivos multijugador alcanzaron su popularidad con el lanzamiento en 2004 del archiconocido *World of Warcraft*. En este, los jugadores asumen el papel de seres de ficción fantástica —enanos, elfos, etc.— que van progresando en

habilidades con el paso del tiempo y el cumplimiento de misiones, además de ir encontrando u obteniendo bienes más valiosos —espadas mágicas, armaduras de gran protección…—. Para jugar, hace falta pagar una cuota mensual, que es la fuente de ingresos de la empresa, con la que se puede acceder a los servidores donde existe el *metaverso*. Algunas personas no están dispuestas a emplear el tiempo que requiere el avance, pero están sobradas de dinero. En países pobres, por el contrario, lo que falta es efectivo que están dispuestos a obtener a cambio de los trabajos más rutinarios del juego. Es decir, se está pagando dinero real por bienes virtuales. La empresa Blizzard Entertainment prohíbe ese tipo de compraventa. Sin embargo, por la naturaleza del juego, permiten y hasta estimulan el intercambio entre personajes. Los que realizan ese tipo de trabajo aprovechan ese medio para pasar productos a cambio de capital común que se entrega a través de PayPal o Western Union.

Quieres realizan esa actividad son conocidos como *granjeros de oro*, que se definen como *aquellos que realizan una repetición de tareas monótonas que proporcionan un beneficio en oro virtual*. Aunque el negocio arrancó en Corea del Sur, se estima que el ochenta por ciento de todos los que se dedican a ese negocio están en China, donde la llevan a cabo en ciberlocales, oficinas o hasta domicilios convertidos en pisos patera. El sueldo que se obtiene es muy superior al medio de las provincias interiores, lo que atrae a los jóvenes a las grandes ciudades. En 2004, coincidiendo con la fiebre por el *WoW*, se disparó la demanda. En algunas prisiones chinas como la de Jixi, los internos, después de agotadoras jornadas de trabajo forzado en el campo, eran obligados a hacerlo frente a la pantalla del ordenador hasta la extenuación. Según declaraciones de los presos, los jefes de la cárcel llegaban a ingresar cada día cantidades cercanas a los mil euros, una fortuna en aquel país.

A medida que los *granjeros* aumentaban y se producía más y más oro y bienes, la inflación, como en el caso de *Ultima Online*, se disparaba. Hasta cierto punto, también la abundancia de objetos mágicos más poderosos. El principal efecto fue que costaba menos dinero real adquirir montañas de oro y equipo. Dejó de ser rentable y la cantidad de *recolectores* cayó en picado, a lo que se sumaron también las acciones proactivas de Blizzard para acabar con ello. Se pudieron llevar a cabo porque hay una empresa detrás que controla las emisiones de oro, hasta el punto de poder despojar a un jugador cualquiera de sus ganancias si sospecha que las ha obtenido de forma ilegal. De esta forma, tener dinero en el *WoW* u otros juegos similares es un riesgo, dado que se puede perder en cualquier momento. De hecho, *Warhammer Online*, por ejemplo, tiene empleados dedicados al borrado de negocios en los que esté implicado dinero real —es decir, pagarle con euros a un jugador para que entregue a otro un hacha virtual—. Otros, como *World of Tanks* de la empresa bielorrusa *Wargaming.net*, tienen su propia tienda virtual, único lugar legal donde se pueden comprar oro y objetos para el juego.

A pesar de todas estas medidas de seguridad y de la prohibición expresa, existen compañías, como IGE, que venden sin pudor y de manera pública bienes de multitud

de juegos. Su presidente estimó en 2006 en casi novecientos millones de dólares el dinero intercambiado anualmente entre jugadores, *granjeros* o no.

En 2016 esta industria pseudolegal pervive de una manera diferente: los ciudadanos ricos pagan a los pobres para que les vendan personajes que ya han alcanzado un nivel de desarrollo interesante, actividad tampoco permitida, por supuesto, en casi ningún juego. Los términos del contrato con la mayoría de empresas avisan que eliminarán de inmediato cualquier personaje que sospechen que ha sido vendido, con lo que se perderá todo el dinero y el tiempo invertido.

Como era de esperar, donde hay sociedad y economía, existe el delito patrimonial. En algunos casos, jugadores veteranos extorsionan a los novatos, muy al estilo del matón de instituto, para que les entreguen parte de su oro a cambio de no matarlos, que convierten en moneda legal de manera inmediata. Si bien los personajes *resucitan ipso facto*, la molestia de ser agredido una y otra vez puede ser tan grande que haga que el juego pierda todo su interés.

En otros juegos hay robo de propiedades, espionaje industrial, piratería y hasta prostitución virtual. Una chica de diecisiete años que se hacía llamar *Evangeline* montó en 2003 un *ciberburdel* en un juego llamado *The Sims Online*, parecido hasta cierto punto a *Second Life*. El término *sim* significa *vida simulada*. Obtuvo una notable cantidad de dinero *sim* que le pagaban a cambio de servicios sexuales tan virtuales como el universo en que se movía, es decir, hablar de sexo y cobrar por ello. Según *Evangeline*, muchas de las chicas que tenía contratadas también eran menores. En ocasiones llegaban a cobrar por servicio hasta el equivalente a cincuenta dólares de la época (quinientos mil *simoleans* que, debido a la brutal inflación, también ahí, hoy valdrían mucho menos). El escándalo fue mayúsculo, con serias reflexiones sobre el límite de la prostitución en general y la de menores en particular, hasta el punto de que quien lo descubrió, un profesor universitario llamado Peter Ludlow, fue expulsado del *metaverso*. No era el único escándalo que había descubierto. Desde su periódico sobre el mundo virtual *Alphaville Herald* —todavía activo, aunque sin actualizar desde 2013— entrevistó a gran parte de la delincuencia simulada, incluso reportó casos de maltrato físico entre hermanos en el mundo real que afirma que fueron ignorados por la empresa creadora del juego, Maxis.

Muchos países están regulando ya las llamadas monedas virtuales. El Banco Central Europeo las define como «un tipo de moneda digital no regulada, que es emitida y controlada por sus desarrolladores y es utilizada y aceptada por los miembros de una comunidad virtual concreta». La Autoridad Bancaria Europea fue un paso más allá y explicó que es «una representación digital de un valor que no es ni emitido por un banco central ni por una autoridad pública ni está necesariamente emparejada con una moneda fiduciaria, pero es aceptaba por personas físicas o jurídicas como método de pago y puede ser transferida, almacenada o intercambiada de manera electrónica». El gobierno de China, por su parte aseguró que «las monedas virtuales, que pueden ser convertidas en dinero real por una cierta tasa de cambio,

solo serán permitidas para comprar bienes y servicios virtuales proporcionados por su emisor, no para bienes y servicios reales». De esta manera prohíbe su uso directo en la economía nacional, pero permite que sean convertidas en yuanes, con lo que obtiene el mismo resultado pero de manera indirecta.

Este tipo de dinero puede categorizarse en *cerrado*, cuando solo puede ser usado dentro del juego, como en el *WoW*, aunque ya hemos visto que se compra y vende fuera del mismo, o *convertible*, cuando hay una tasa de intercambio con el mundo real, como los dólares Linden que hemos mencionado.

Todas las economías que hemos descrito hasta ahora, todas estas monedas virtuales, con sus fluctuaciones, no son útiles para los grandes delincuentes, aunque han sido utilizadas por ellos como una manera más de dificultar su rastreo. Como veremos en el capítulo siguiente, los autores del temido virus de la policía utilizaban dólares Linden como parte de su estrategia de blanqueo. Son monedas que dependen de una autoridad central —la empresa emisora— con un amplio margen de maniobra para eliminar movimientos sospechosos. Por ello hace falta algo más. Una divisa descentralizada que no controle nadie. ¿Es posible?

EL DINERO QUE NADIE EMITE Y TODOS ACEPTAN

El dinero apareció ya en la prehistoria, cuando el hombre dejó de ser nómada y los asentamientos estables, agrícolas y ganaderos, empezaron a producir excedentes que podían ser intercambiados por otros de los que se encontrasen faltos. Por ejemplo, un agricultor podría cambiar trigo por queso de oveja. Este sistema evolucionó al dinero-mercancía. Una serie de bienes que, además de su uso tuvieran un valor intrínseco que pudiera servir de patrón para el intercambio. Siguiendo con la propuesta anterior, dos medidas de trigo equivalen a un hacha de bronce, lo mismo que un queso del tamaño de un puño. De esta forma, se puede intercambiar el instrumento, que además no es perecedero, en vez de promesas de restituir el bien intercambiado. Es decir, como el trigo no se siega a la vez que el queso acaba su curación, en vez de acordar que el uno se entregará a cambio del otro, el dinero-mercancía, el hacha de bronce, sirve como pagaré o justificación. No es extraño encontrar en yacimientos arqueológicos tesoros enterrados que consisten en decenas de ejemplares de esa herramienta.

No tardó en sustituirse por metales escasos y no perecederos, en especial el oro y la plata, que no eran manufacturas complejas y eran más fáciles de transportar y valorar. El siguiente paso lógico fue marcar los lingotes, de un peso determinado y pronto de forma más o menos redondeada, lo que se dio en llamar *moneda*.

El primer cambio importante lo constituyó el papel moneda, los billetes bancarios, primero emitidos en China a partir del siglo VII. Un trozo de pasta de celulosa impreso no tiene valor por sí mismo, pero queda respaldado por la promesa

de un pago en el metal equivalente por parte del Estado correspondiente. Esto es, en teoría, que con un billete se puede acudir al banco nacional y pedir que se entregue la cantidad correspondiente en oro. Eso se llamó *patrón oro* y estuvo vigente en Europa hasta después de la Segunda Guerra Mundial. Cada moneda correspondía a un valor fijo de oro almacenado en los depósitos nacionales, por lo que su precio y la relación con otras divisas eran más o menos fijos. Cualquier ciudadano podía exigir que le cambiaran el billete por los gramos de metal indicados.

Este sistema tuvo varios altibajos entre la Primera y la Segunda Guerra Mundial, momento en que dejó de servir. En esa convulsa época de crisis, los países necesitaban más dinero del oro que disponían para mantener la muy costosa maquinaria bélica. Comenzaron a imprimir billetes con valor futuro, es decir, no convertibles a voluntad del ciudadano, sino del Estado. Después de la paz de 1945, el patrón oro se modificó. Solo el dólar estadounidense sería convertible en oro, con las reservas que aquel país mantenía en Fort Knox. Las demás divisas tenían una equivalencia fija con aquel, dado que el dinero seguía representando un valor en oro, aunque fuese a través de un intermediario.

Nixon acabó con ese modelo en 1971, cuando las necesidades de fondos para Vietnam le forzaron a emitir más papel del que podía respaldar. Ese fue el momento de la última gran revolución. El dinero se convirtió en *fiduciario*, esto es, no tiene más valor que el que sus propios usuarios le quieren dar, un valor *de confianza mutua*. El intercambio de bienes a través de papel moneda o equivalente electrónico —cada vez más las transferencias se realizan de banco a banco, modificando apuntes contables en uno y otro, sin que haya un envío físico en forma de billetes— es un acuerdo entre ciudadanos y países, basado en equivalencias que varían de forma continua. Si una nación necesita más efectivo puede imprimirlo a voluntad, pero eso va a causar que los precios aumenten dentro de las fronteras —inflación— y que la moneda valga menos en el exterior —devaluación—, es decir, que por una divisa determinada se obtienen menos de las de otros países. Hay que mantener una armonía muy delicada para que la economía no se desmorone ni los desequilibrios entre regiones del globo acaben con el sistema, porque todo está sustentado tan solo por algo tan volátil y difícil de calcular como la confianza entre las partes. Por eso, si el mercado internacional disminuye la seguridad en una moneda —piensan que el estado que la respalda no va a ser capaz de afrontar sus gastos—, esta pierde parte de su valor (los demás países dan menos monedas propias por la divisa en duda). Del mismo modo, si los propios ciudadanos no creen en ella, van a pedir otra —algo típico en países como Argentina, lo que desembocó en el famoso *corralito*— o una cantidad muy alta por un mismo producto, con lo que los precios —la inflación— se disparan.

En la situación actual hay productos seguros, que disponen de una gran apreciación y que, en caso de colapso, seguirían sirviendo, como los metales preciosos y otras sustancias que proceden de la minería. Su escasez y su utilidad van

a darles un valor intrínseco en cualquier sociedad compleja (por supuesto, si todo va mal y volvemos a una economía básica de subsistencia como la del Paleolítico, lo único que valdrá de algo serán los bienes inmediatos: alimentos, utensilios, hogar y ropa).

En 2008, un grupo que hasta hoy permanece en el anonimato y que se hace llamar Satoshi Nakamoto publicó en una lista de intercambio de correos sobre criptografía llamada *Meltzdowd.com* un artículo sobre una moneda de total seguridad que estaría fuera del control de cualquier gobierno a la que denominó Bitcoin y que lanzaría al mercado el 3 de enero del año siguiente. Varias personas, entre las que destaca el australiano Craig Steven Wright, han afirmado estar detrás del pseudónimo, pero hasta el momento ninguna afirmación ha resultado creíble.

La moneda, al contrario que el resto de las actuales, no es fiduciaria en el sentido común del término. Cada una representa un esfuerzo de computación, con sus gastos en electricidad y otros servicios asociados, como explicaremos más adelante. Por ello el proceso de generarlo se llama, con una analogía muy gráfica, *minería*. De hecho, hay estudios de las universidades de Oxford y Warwick que han definido su comportamiento como más parecido a los metales preciosos que a las divisas.

Otra importante diferencia con el dinero tradicional es la ausencia de una autoridad central que controle las transacciones que se realizan. Salvo para los pagos en mano, que son los menos, si un ciudadano desea entregar a otro una cantidad de dinero físico, esta transferencia pasa por una entidad bancaria que comprueba la validez de la misma y la hace llegar a su destinatario; ejerce de mediadora y puede revertir el envío si el emisor lo solicita y se cumplen una serie de parámetros. Las diferentes legislaciones, con muy pocas excepciones, requieren que ambas partes estén identificadas y los gobiernos pueden fiscalizar las cuentas. Se puede evitar estableciendo contacto directo entre quien paga y quien cobra. Para ello no se puede utilizar moneda corriente, porque todo en ellas está controlado hasta el extremo. La opción es crear una divisa que solo exista de manera virtual, en ordenadores y redes informáticas, en vez de estar impresa o almacenada en bancos.

El primer problema que presenta es que los datos informáticos pueden ser copiados con facilidad. No hay forma de saber si existen una o mil copias de un archivo cualquiera, a menos que lo podamos asociar de forma única a quien lo envía y a quien le llega. Dicho de otra manera, se debe evitar el doble pago, que una persona pueda emplear la misma Bitcoin para pagar dos veces. Por tanto, hay dos partes de un mismo asunto a solucionar, evitar la copia y que las transacciones sean únicas, sin vuelta atrás. La solución que Nakamoto propuso está basada en una red entre iguales (*peer to peer*) cuyos datos tengan naturaleza criptográfica.

La criptografía está lejos incluso de modelos tan avanzados como lo fue en su día la máquina Enigma que utilizaban los alemanes para cifrar sus comunicaciones en la Segunda Guerra Mundial y que fue vulnerada por los Aliados al principio de la contienda, gracias al trabajo de un grupo de matemáticos entre los que destacó Alan

Turing, padre de la computación moderna. Por entonces, uno de los principales esfuerzos consistía en que el enemigo no supiera cómo se codificaban los mensajes, que el algoritmo fuera secreto. Hoy no se considera seguro ningún método de encriptación cuya forma de calcularse no sea conocida y haya sido puesta a prueba por los expertos en seguridad de todo el mundo. A la hora de proteger un archivo informático cualquiera, los programas capaces de hacerlo (PGP, Criptod, AxCrypt y otros muchos) generan una clave aleatoria basada en algún tipo de evento (la hora del ordenador, un nombre tecleado o el lugar donde se hace clic con el ratón, por poner solo tres ejemplos) que se aplica a una fórmula matemática que ya es conocida. Como el dato con el que se aplica el cálculo es desconocido, el resultado final, lo que hace falta para *reventar* la seguridad, es también desconocido. Eso no quiere decir que sea del todo invulnerable. Para descubrir cualquier clave solo hacen falta dos cosas, tiempo y ordenadores. Cuando el primero, a pesar de disponer de muchos de los segundos, se calcula en años o siglos, la clave se considera segura. Como la computación avanza de forma exponencial, lo que hoy está a salvo puede ser descubierto con facilidad dentro de una década.

Existe una forma todavía más sofisticada de encriptar, llamada asimétrica, muy útil cuando hay que enviarlo a terceros. El algoritmo crea para cada usuario una clave en dos partes, una pública y una privada, relacionadas de forma unívoca. La pública de cada uno es conocida por todos los miembros de la red y, de hecho, debe serlo para que puedan hacer llegar un mensaje a un destinatario concreto. El emisor de un mensaje determinado tiene que utilizar entonces la clave pública de su receptor y aplicar el algoritmo. El resultado se envía a su destinatario, que es el único que va a poder descifrar su contenido, utilizando para ello la clave privada. Si, por el contrario, un emisor usa esta para cifrar un mensaje, cualquiera que disponga de su clave pública podrá obtener su contenido. Esto se conoce como *firma digital*, dado que solo el poseedor de la clave privada —salvo que se la hayan robado— puede haber emitido ese mensaje, con lo que la autenticidad del mismo queda probada. Por supuesto, en una firma digital no se comunica cuál es la clave privada —o dejaría de ser privada—, sino que se informa de que se ha cifrado con ella, y así quien posea la pública puede acceder y verificarlo.

En la criptografía moderna no hay que entender estas claves como palabras al uso, sino que son largos segmentos de caracteres numéricos, alfanuméricos y en ocasiones, símbolos, casi imposibles de recordar para un humano, por lo que son los programas *ad hoc* los que las conservan en sus memorias.

Cualquier envío de Bitcoins se define como una suma criptográfica que va firmada digitalmente por el emisor y que incluye la clave pública del receptor. Un conjunto de clave pública de uno y firma —con la clave privada— del otro, más las Bitcoins contenidas en ella es lo que se denomina un *monedero*, que es gestionado por alguno de los muchos programas gratuitos. Estos monederos pueden estar en posesión física de su dueño —en un ordenador o en una memoria USB, por ejemplo

— o bien en un servidor remoto —en la nube—. Su pérdida bloquearía de forma efectiva todo lo contenido en él, pero no lo eliminaría del sistema, que está limitado a un total de veintiún millones de Bitcoins de los que a finales de 2015 ya había emitidos quince. Este sistema cerrado, la imposibilidad de superar el techo, va a causar que nunca exista inflación, aunque, como veremos más adelante, la fluctuación con las monedas físicas es muy elevada.

El problema, recordemos, es cómo evitar que se envíe una misma cantidad a dos personas o más, es decir, conseguir que un dinero determinado solo se gaste en una ocasión, dado que el poseedor de una cifra criptográfica que represente una determinada cantidad puede hacer varias copias de ella.

Los creadores decidieron establecer una red de usuarios que voluntariamente se dedicasen a mantener la llamada *cadena de bloques*, una estructura que mantiene un registro cronológico de todas las transacciones llevadas a cabo en la red. De esta manera, si un gasto determinado está registrado a las 14.33 horas, no puede volverse a enviar a las 14.34. En caso de que un usuario malicioso enviase ambos gastos en el mismo instante —algo que es más un caso teórico que real—, solo el que entrase primero en la cadena de bloques se consideraría válido. Cada transacción, por tanto, está marcada por el emisor con su clave privada (firma) y la clave pública del destinatario, y tiene una marca de tiempo. El receptor, además de recibir un mensaje con la transacción, debe comprobar que la misma ha sido verificada por la cadena de bloques. Esto ocurre en la actualidad en unos seis minutos. Hasta que no ocurra no debería darse por buena. Supongamos que un delincuente ha realizado dos compras con la misma moneda y cada comerciante recibe el mensaje de que la transferencia se ha realizado, aunque todavía no la confirmación. Ambos envían la mercancía al estafador. Uno de ellos recibirá el pago verdadero, mientras que el segundo recibirá el mensaje de que su venta no se ha realizado, puesto que la Bitcoin ya está en poder del que primero ha entrado en la lista.

La cadena de bloques, por tanto, es el conjunto de todas las transacciones de Bitcoins efectuadas en todo el mundo, guardada, a su vez, mediante una serie de combinaciones criptográficas que realizan de forma continua las máquinas que pertenecen a la misma —llamada *proof of work* o prueba de trabajo—. La mayoría de usuarios solo tiene un monedero —o varios— que cargan y vacían, pero no pertenecen a la red de voluntarios que mantiene la cadena y a la que cualquiera puede apuntarse y borrarse en cualquier momento e incluso puede hacerlo de manera intermitente. Cada miembro debe solucionar un problema matemático en un tiempo determinado —un paso de la cadena de bloques—. Si lo consigue, recibe un premio en forma de Bitcoin. Todos los miembros de la red compiten para resolver un bloque, pero solo el primero que lo consiga va a obtener la recompensa, que en la actualidad son veinticinco Bitcoins, cerca de doce mil dólares. Este proceso de llama *minería* y es la única manera de generar nuevas monedas. Al principio, cada solución podía alcanzarse por un ordenador doméstico cualquiera. En la actualidad suelen asociarse

muchos usuarios para trabajar en común, cada uno con una pequeña fracción del problema para luego repartirse los Bitcoin que ganan. Debe hacerse tan rápido que ningún ordenador individual tiene hoy la capacidad de resolver por sí mismo un caso. Cuando muchos nodos se conectan, se llega a un límite en que el incentivo recibido apenas compensa el gasto de electricidad efectuado para conseguir el premio, en especial teniendo en cuenta que solo el primer equipo que lo consigue cobra, y todos los demás pierden el esfuerzo realizado, que es intenso en recursos de computación. En esos casos, el número de participantes disminuye, por lo que es más fácil completar la tarea y ganar las Bitcoins y eso incentiva a otros a volver a la red. De esta manera, la red de cadena de bloques se regula por sí misma. En cualquier caso, cuando se alcance el tope de veintiún millones, suponiendo que el sistema siga existiendo para entonces, las recompensas cambiarán a una comisión por cada transferencia introducida en la cadena de bloques. Las veinticinco Bitcoins se deducirán de todas las transferencias que formen cada bloque. Así sigue existiendo un incentivo para que los voluntarios continúen prestando sus ordenadores al sistema.

La prueba de trabajo que sella cada paso de la cadena de bloques tiene el propósito de evitar un ataque a la misma. Si un ordenador o pequeño grupo puede sustituir un trozo de la cadena e introducir una falsificada por ellos, pueden aparecer o desaparecer pagos a voluntad, con lo que todo el método Bitcoin se convierte en poco menos que inútil. Sin embargo, para hacer tal cosa hay que duplicar todo el trabajo desde el punto en que quiera introducir su modificación, puesto que cada paso va asociado al anterior de forma unívoca. Habría que repetir todo el proceso desde el instante en que se quisiera modificar un pago hasta el presente, algo que avanza a gran velocidad, puesto que la moneda está en continuo movimiento y una nueva transacción solo puede hacerse cuando la recepción de la anterior ya ha sido confirmada. Por tanto, el atacante tendría que tener una potencia de proceso superior a todos los ordenadores que forman la red *juntos* para mantener una cadena de bloques equivalente. La posibilidad técnica existe, aunque requeriría tal esfuerzo económico que no resultaría rentable. Costaría más la inversión a realizar que el beneficio obtenido. La llegada en un futuro de ordenadores cuánticos que multipliquen por miles la capacidad de los actuales puede poner todo esto en entredicho, al menos durante un tiempo, pero ese escenario aún parece lejano.

En resumen, el funcionamiento de la red que mantiene Bitcoin es el siguiente:

1. Cada transacción de dinero entre dos miembros de la red se transmite a todos los ordenadores o grupos —llamados *nodos*— que trabajan en la cadena de bloques.
2. Cada uno de los nodos coge todas las transacciones recibidas en un periodo determinado y crea un bloque con ellas.
3. Cada nodo comienza a realizar los complicados cálculos criptográficos que forman la prueba de trabajo y aseguran el bloque.
4. El primer nodo que consigue resolver una prueba de trabajo la envía a todos los

miembros de la red.
5. Si todas las transacciones que forman el bloque son válidas y una misma moneda no se ha enviado a dos personas diferentes, todos los nodos aceptan el bloque como válido y quien lo ha resuelto recibe su recompensa.
6. Los ordenadores de la red marcan ese bloque como el válido y comienzan a calcular el siguiente, que tiene que ir por fuerza a continuación del anterior.

Existe un sitio web oficial conectado al sistema, *blockchain.info*, donde cualquier internauta puede observar en tiempo real las transacciones que son comunicadas a la red y los bloques que se están resolviendo con ellas. Por ejemplo, el 30 de abril de 2016 se solucionó, entre otros muchos, el bloque que hacía el número 409 867 desde el comienzo del sistema. Incluyó más de dos mil doscientas transacciones y el cálculo de la prueba de trabajo reportó a un equipo georgiano conocido como BTCC Pool unos beneficios de unos once mil trecientos dólares al cambio de ese día, que se dividieron entre todos los miembros de la red. El bloque anterior, sin embargo, solo contenía novecientos setenta y tres envíos de dinero, aunque el trabajo criptográfico fue similar, así como la ganancia, que fue para unos austriacos.

El sistema funciona y es tan estable que Bitcoin ganó pronto una notable aceptación popular, a pesar de que el propio equipo que lo gestiona afirma que sigue en pruebas y aconsejan no utilizarlo para guardar ahorros, puesto que su volatilidad es altísima y, al carecer de autoridad alguna que lo modere, sumado a su cantidad relativamente baja —es más fácil influir en siete mil millones de dólares, capitalización de las Bitcoins, que en diecisiete billones, PIB de Estados Unidos—, está sujeto a ataques financieros, fluctuaciones y hasta a la simple pérdida de confianza de sus usuarios. Eso quiere decir que de un día para otro puede valer un diez por ciento de lo que costaba o que deje de haber suficientes nodos conectados y sea posible vulnerar la seguridad de la cadena de bloques.

Bitcoin, lanzado en enero de 2009, logró su paridad con el dólar en mayo de 2011. Hasta entonces había estado muy por debajo. Ese junio tuvo su primer pico, cuando se puso en treinta y dos dólares —coincidiendo con el conocimiento para el gran público de Silk Road, que solo aceptaba pagos con ella—, aunque cayó de inmediato a unos dieciocho y continuó un suave descenso hasta fin de año, cuando apenas duplicaba a la divisa estadounidense. Siguió una suave progresión ascendente hasta la primavera del 2013, cuando superó los doscientos dólares para luego mantenerse estable en torno a los cien. Una minucia en comparación con lo que ocurriría a comienzos de 2014, donde alcanzó su máximo histórico de ¡1151 dólares por cada Bitcoin!, para de nuevo tener una brusca caída, debido a la quiebra de uno de los principales portales de cambio entre moneda estatal y privada, Mt. Gox, que reconoció que le habían robado 750 000 Bitcoins, un siete por ciento del total existente entonces, valoradas en casi quinientos millones de dólares. Desde entonces hasta 2016 ha fluctuado en torno a los cuatrocientos dólares.

Esta primera moneda virtual no ha tardado en tener una colección de clones que funcionan de manera muy similar, implementando en la mayoría de ocasiones el mismo sistema de seguridad y verificación por cadenas de bloques. Algunas de las divisas más conocidas son Ethereum, Litecoin o Syscoin. Otras apenas tienen movimiento, con un tráfico mundial diario no superior a los cien dólares, como Ixcoin o CasinoCoin.

ENTRE EL MUNDO FÍSICO Y EL VIRTUAL

Hemos generado mediante *minería* varias Bitcoins o bien deseamos gastar algunos euros para tener efectivo virtual. ¿Cómo cambiamos entre ambos tipos de divisa? Lo más sencillo es acudir a un agente de cambio como CoinDesk, Bitstamp, Bitfinex, Coinbase, itBit u OKCoin. Eso sí, debemos ser conscientes de que en cuanto haya moneda nacional de por medio, un banco va a saber de nuestros ingresos o gastos y se acaba el anonimato. Como no hay nada ilegal en ello en España, si las cantidades son pequeñas, vamos a pasar desapercibidos. Lo que hagamos después con la criptomoneda nadie lo podrá saber hasta que no volvamos a capitalizarla.

La tasa de cambio global para los principales operadores puede verse, por ejemplo, en la página *coindesk.com*. Todos ellos presentan una fluctuación muy similar, es decir, el cambio a nivel mundial tiene una variación muy escasa, da igual el lugar del globo en que uno se encuentre.

La consideración de las monedas virtuales está sujeta a mucha controversia. Su falta de control —por otro lado, el sueño de cualquier economista liberal— la hace ideal para utilizarla en el mercado negro. De hecho, como vimos en el capítulo quinto, son la única divisa válida en los bazares oscuros de la *deep web*, algo en lo que su anonimato tiene mucho que ver. Para gestionar las criptomonedas no hace falta identificarse de manera alguna. Crear monederos es gratis, basta con descargarse un programa que lo solicite, y las transferencias se hacen entre esos dispositivos. Los intercambios se pueden hacer dentro de redes como TOR, que garantizan que nuestra verdadera dirección IP no va a poder ser detectada con facilidad. Los creadores de Bitcoin explican que el único dato rastreable que se envía a la cadena de bloques es la identificación del monedero emisor y del receptor. Por eso recomiendan crear uno nuevo para cada operación. Eso es algo que tienen muy en cuenta los fanáticos de la seguridad, bien por convicción, bien porque la naturaleza de su actividad es ilegal. Con la popularización de las criptomonedas, que están llegando al público general, cada vez más usuarios no consideran necesaria esa medida de seguridad, puesto que no hacen nada ilegal o no tienen constancia de ello, como muchos de los compradores de drogas en sitios como Alphabay o Nucleus.

Las divisas digitales son un producto nuevo que avanza más rápido que la legislación que lo debe regular, como es habitual en el mundo de la tecnología. Los

gobiernos miran por tres aspectos principales: la compra de bienes ilícitos de forma subrepticia, el blanqueo de capitales y la evasión de impuestos. Es muy difícil detectar movimientos de un capital que, por su propia naturaleza, es descentralizado. Los esfuerzos deben dedicarse al momento en que las monedas virtuales son convertidas en físicas. En la Unión Europea los bancos están obligados a informar a Hacienda de los movimientos de capital superiores a tres mil euros, pero resulta fácil a un delincuente dividir sus millones en fracciones inferiores que puede mover entre varias cuentas bancarias diferentes, que incluso pueden haber sido creadas por *muleros* —recordemos el capítulo anterior—. En la información oficial sobre Bitcoin se explica que sus beneficiarios deben declarar sus ganancias de la misma manera que lo harían con cualquier otro capital. Que hagan caso o no, por supuesto, depende de la voluntad de cada ciudadano.

Las divisas digitales aún están sin regular en la mayor parte de países. Algunos han decidido, al menos por el momento, prohibir por completo su uso, como Bolivia, donde su banco central prohibió «el uso de toda moneda no emitida o regulada por estados, países o zonas económicas» el 6 de mayo de 2014. Rusia, de manera parecida a China, solo permite comprar bienes en su país con rublos, aunque es legal almacenar, ganar o cambiar dinero digital. De hecho, es uno de los lugares en que su uso es más popular.

La Hacienda de Estados Unidos decidió el 25 de marzo de 2014 darles la consideración de bienes muebles, no de dinero. De esta manera, sus poseedores deben tributar por ellas como ganancias de capital y, al mismo tiempo, ganan seguridad jurídica. Ya saben a qué atenerse.

La Unión Europea estudia prohibir transferencias de criptomonedas desde o hacia países *de alto riesgo*, en un esfuerzo de dificultar las finanzas de grupos terroristas como los que atentaron en París en noviembre de 2015 o en Bruselas de marzo de 2016. Aunque algunos estados, como Alemania, las reconocieron en 2013, en la legislación de la Unión siguen en un limbo jurídico, en parte azuzado por el miedo a una economía global descentralizada y sobre la que no puedan ejercer control alguno.

El juego continúa. Para facilitar todavía más la labor a los ciudadanos, se están instalando por las calles de las ciudades de España cajeros automáticos para comprar y vender Bitcoins. En el centro comercial ABC Serrano de Madrid o en la estación de trenes de la Plaza de España de Barcelona su presencia ya no sorprende a los viandantes. En ellos se pueden introducir billetes de cinco a veinte euros con los que cargar un monedero virtual que se suele llevar en el teléfono por comodidad —con lo que se evita una identificación por parte del banco en que se tenga el dinero al realizar una transferencia a un agente de cambio—. En un paso más, existen varias empresas que permiten llevar Bitcoins físicas en el bolsillo, que tienen diferentes formas y aleaciones. Cada usuario solo tiene que grabar la clave pública y privada —la primera, legible con un código QR, la segunda, oculta a la vista— para disponer de un efectivo tangible.

Aunque las criptomonedas afirman ser seguras y anónimas, no son invulnerables. Como vimos al hablar de Silk Road, al intervenir los monederos en los que *CronicPain* y, sobre todo, el cabecilla, *Dread Pirate Roberts*, guardaban sus Bitcoins, sitos en sus ordenadores, pudieron ser incautadas por el FBI y luego subastadas. La tentación de apropiarse de algunas también fue demasiado grande para el agente del Servicio Secreto Shaun Bridges, que acabó condenado en sentencia firme por ello. Hubo otro arresto relacionado con las criptomonedas y la Ruta de la Seda. En enero de 2014 se detuvo en el aeropuerto de Nueva York, cuando volvía de un congreso en Ámsterdam, a Charlie Shrem, presidente de la compañía BitInstant, que se dedicaba a hacer de intermediaria para pagos en Internet. Ante cualquier compra, se accedía a su web —hoy desactivada— y se pagaba en *dólares*. Ellos compraban las Bitcoins equivalentes y enviaban la cantidad al destinatario, que de esta forma no tenía necesidad de poseer un monedero. Lo que llevó a su jefe a la cárcel de Lewisburg, en Pensilvania, es que estaba utilizando sus recursos para blanquear hasta un millón de dólares del bazar ilegal. Aceptó una condena de dos años por esos cargos.

El escándalo más grande, que ya hemos mencionado antes, fue el cierre de la casa de cambio japonesa Mt Gox en febrero de 2014, mientras gestionaba el siete por ciento de todas las Bitcoins existentes. Desde su apertura en Tokio en 2010, creció en popularidad hasta conseguir hacerse con el setenta por ciento de todo el mercado. A lo largo de su breve existencia tuvo varios problemas. El primero y más notorio fue un ataque de un *hacker* que consiguió infiltrarse en los ordenadores de la compañía en junio de 2011 e hizo caer la cotización interna a un centavo —con lo que cualquiera que realizase una transacción con ellos iba a obtener muchos Bitcoins casi gratis—. La intrusión se detectó en cuestión de minutos y parece que el agresor no consiguió su objetivo.

Algunos meses después, en octubre, se emitieron órdenes de transferencia de más de dos mil seiscientas Bitcoins a cuentas inexistentes. Los operarios de Mt. Gox no se dieron cuenta —cualquier usuario particular hubiera sido consciente del error y lo habría cancelado— y los envíos entraron en la cadena de bloques, con lo que el dinero se perdió de forma irrecuperable.

La debacle llegó en febrero de 2014, cuando anunció la suspensión de actividades y la quiebra, debida, en parte, a la desaparición de tres cuartos de millón de criptomonedas. Un mes después encontró doscientas mil en un monedero que llevaba inactivo desde 2011. En un principio no estaba claro si se debía a un robo, una estafa o a una simple mala administración. Un estudio de los expertos en seguridad de Bitcoins WizSec concluyó que se había debido a la sustracción continuada y sistemática de fondos de la empresa, que empezaron en 2011. En ningún caso se comprometió el sistema de funcionamiento de Bitcoin, que sigue siendo robusto y seguro, sino que el ataque se dirigió contra los ordenadores de una compañía concreta.

La cadena de bloques tiene una seguridad y versatilidad tan grande que, con las

adecuadas correcciones, algunas voces ya aseguran que podrá incluso suplantar muchas de las funciones que hoy cumplen los notarios, puesto que puede *dar fe* del acuerdo entre dos personas que, una vez introducido en el sistema, quedará sellado y rubricado.

La perspectiva actual nos dice que las criptomonedas han llegado para quedarse. Es muy posible que en los años venideros las veamos expandirse y crecer, tanto en capacidades como en cuota de mercado, a una escala que no podemos imaginar, del mismo modo que un usuario de un móvil de 1995 no podía siquiera concebir uno de los actuales teléfonos *inteligentes*.

8

HACKERS: EL ARTE DE LO POSIBLE

Manu y David trabajan en la Brigada de Investigación Tecnológica de la Policía Nacional. Es 2010, están en la azotea de un hotel de lujo de Palma de Mallorca y no acaban de creer lo que sus sistemas de escucha electrónica están captando, un auténtico bombardeo de ondas con un propósito muy concreto y dañino.

El establecimiento había cambiado hacía poco más de un mes de proveedor de servicios de Internet. El nuevo, una empresa pequeña que estaba empezando, les había garantizado un mejor servicio, con WiFi de gran velocidad en todas las habitaciones, por un precio más que competitivo. Sin embargo, algo salió mal. Después de unos días en que la dirección se congratulaba del avance, el sistema dejó de prestar servicio. Ningún cliente podía conectarse a Internet desde sitio alguno. Hasta la red física, la que tenía cables, iba lenta o no iba en absoluto. Los técnicos acudían una y otra vez y comprobaban que todos los instrumentos funcionaban. No parecía haber ninguna intrusión ni virus en los equipos, que incluso cambiaron. Alguna vez pareció funcionar durante algunos minutos y luego volvió a las andadas. Lo único anormal era una cantidad de peticiones de conexión inusuales por su número. En un principio lo atribuyeron a los usuarios que intentaban con desesperación conectar, hasta que quedó patente que lo que estaba pasando era demasiado hasta para unos huéspedes hiperactivos. Había un ataque, pero no sabían cómo y les estaba costando clientes. Por eso lo denunciaron y, una semana más tarde, dos expertos de la BIT se desplazaron desde Madrid para tratar de arrojar algo de luz al caso. En cuanto accedieron a los routers comprobaron que cada segundo había cientos de solicitudes de conexiones a esa WiFi, como si toda la ciudad quisiera y no consiguiera utilizar Internet desde el establecimiento. Entre ellas, los accesos legítimos eran una gota en un océano. El sistema intentaba responder a las peticiones de una en una, pero estaba saturado por las falsas.

Como la anterior hipótesis era imposible, para empezar porque el alcance de la señal es limitado, más para los equipos domésticos, tenía que ser alguien con potencia de emisión y malas intenciones. Por eso estaban esa agradable mañana en la azotea con antenas direccionales conectadas a sus ordenadores, donde tenían programas, llamados sniffers, que capturaban todos los paquetes de datos que hubiera en el aire. Después de llevar recorridos apenas cuarenta grados, David dio un respingo. El sensor se había salido de la escala. No fue el único. Detectaron dos lugares más. En la dirección de todos ellos había hoteles de diferentes cadenas. Un ataque coordinado de esa magnitud no parecía lógico, mucho menos para que competidores se pusieran de acuerdo entre sí para fastidiar a un tercero. Ni para robarles clientes.

Los agentes se desplazaron a cada uno de los centros e incautaron antenas enfocadas a la víctima. Utilizaban parte de los anchos de banda de cada sitio para esta acción, de forma que, en conjunto, la conexión de cada hotel seguía prestando servicio. Quien lo había hecho era un experto informático. Uno solo, puesto que los programas y aparatos eran los mismos en los tres emisores. Cuando desconectaron el último, por fin el denunciante pudo volver a proporcionar servicio de Internet.

El autor, detenido poco después, era el anterior prestador de servicios del hotel, que había perdido ante la oferta de la nueva empresa telemática. Para más escarnio, estaba formada por gente que habían sido sus empleados en el pasado. Había decidido escarmentarles para que ningún otro cliente siguiera sus pasos. Pasó su primera noche en el calabozo antes de tener que responder ante un juez y ante los abogados de ambas firmas —hotelera e informática— por su mal perder.

CABALLOS DE TROYA: CUANDO EL PEQUEÑO USUARIO ATRAE LA ATENCIÓN

Si nos ponemos a hablar de seguridad informática, estas líneas se hacen cortas. Una enciclopedia de doce volúmenes sería necesaria para intentar profundizar un poquito. En estas escasas páginas solo vamos a explicar los conceptos elementales con algunos ejemplos reales.

Como vimos en el primer capítulo, vivimos en un mundo conectado que solo va a ir a más con el llamado «Internet de las cosas». La domótica se impone. Todos los electrodomésticos de la casa van a acceder a Internet para llamar al servicio técnico por sí mismos si se averían o encargar aquello que falte en la nevera, por poner dos ejemplos sencillos y que ya están aquí. Por supuesto, los ordenadores ya llevan muchos años en la red y las tabletas y teléfonos se han unido hace algún tiempo.

Ya sabemos que, en cuanto existió una red, allá por los sesenta, se creó el primer virus que tuvo que ser perseguido a conciencia y eso que era solo un experimento. Si existe el canal, alguien va a crear el vehículo. Cuando los ordenadores domésticos no estaban conectados a ningún sitio los *bichos* se transportaban en disquetes, de manera inadvertida. Un ordenador infectado copiaba su infección en soportes externos sin que resultase visible salvo a los más expertos. Cuando ese disco se introducía en otro equipo, la infección se propagaba. Aquel *malware* era más inocente que el actual. Podía ser muy destructivo y, de hecho, en algunos casos podía acabar con toda la información almacenada, pero no había un plan organizado detrás. Era más una demostración de capacidades malignas, como el español *Barrotes* de 1993, creado por alguien que se hacía llamar *OSoft* y que, el 5 de enero se activaba, mostrando una serie de barras verticales en el monitor y borrando la parte del disco duro donde se guardaba toda la estructura del mismo, que de esa forma quedaba inservible.

En 1999 apareció *Melissa*, creado por el estadounidense David Smith. Infectaba

documentos del procesador de textos Microsoft Word y se enviaba a sí mismo a otros contactos de la víctima utilizando su propio correo electrónico. Dependiendo de las variantes, el número de envíos variaba entre diez y ciento cincuenta. Su propagación fue tan masiva que se calculó que un veinte por ciento de todos los sistemas operativos Windows del mundo resultó infectado. Empresas como Microsoft o IBM se desconectaron durante un tiempo de Internet para evitar el daño que causaba. Los estimados en la industria se estimaron en más de ochenta millones de dólares. Todo eso sin destruir datos como hacían los que hemos mencionado más arriba. El departamento de seguridad de la empresa de servicios de Internet America On Line, que entonces dominaba el mercado de aquel país, consiguió rastrear el origen del virus hasta el teléfono de su creador, que fue detenido y aceptó una condena de veinte meses en prisión —del total de diez años que le habían sentenciado en primer lugar— y dos multas por un total de siete mil quinientos dólares. Explicó que el nombre se lo había dado en honor a una bailarina de *strip-tease* de la que se había enamorado.

La novedad de *Melissa*, luego copiada mil veces —como el filipino *I love you* que infectó cincuenta millones de ordenadores en el año 2000—, consistió en que necesita la colaboración de la víctima para lograr su propósito. El virus llegaba en un correo electrónico con un título sugerente como «mensaje importante de Fulanito» —el nombre del infectado— y el texto: «Aquí tienes el archivo que me pediste. No se lo enseñes a nadie». El incauto que abría el documento adjunto se contagiaba y se convertía en el siguiente en esparcirlo.

Solo hay dos maneras de conseguir infectar un ordenador: mediante técnicas de ingeniería social o aprovechando vulnerabilidades de los sistemas operativos. La primera, por mucho, es más fácil que la segunda y necesita de menos conocimientos de programación. Un verdadero *hacker* despreciaría a quien las use pero, para muchos, a la hora de conseguir un objetivo determinado cualquier método vale. En el capítulo seis hablamos del término *phishing*. Hoy, como vimos, es un sinónimo de estafa que consiste en engañar al incauto para que proporcione sus claves de banca telemática. Cuando apareció el término en los años noventa en la red más importante de los Estados Unidos, America On Line, definía una forma de engañar a la víctima para que entregase las contraseñas que usaban para conectarse. Para ello solían hacerse pasar por un trabajador de la compañía y mandaban mensajes privados del estilo «verifique su conexión de forma inmediata». De esta forma, el delincuente lograba hacerse con la cuenta del inocente —así conectaba él en vez de hacerlo el legítimo usuario— y, además, conocía cuál era la tarjeta de crédito que se usaba para pagar por la conexión. El perjuicio era doble. Esto fue tan frecuente que la empresa empezó a mandar avisos continuos en que explicaba que ninguno de sus empleados iba a requerir jamás las contraseñas. Es un ejemplo de fallo de seguridad informática para el que no hace falta ningún programa dedicado, solo paciencia y dedicación.

Un mundo interconectado, por tanto, no representa solo posibilidades de que los virus se propaguen de ordenador en ordenador (de infectado a infectado), sino algo

más interesante, que el aparato de la víctima se ponga en contacto con el del agresor y le comunique todo lo que le parezca importante, como contraseñas bancarias o documentos, o que capture las emisiones de la cámara web. Es el mismo concepto del *phishing* de American On Line llevado un paso más allá. Para ello se inventó un nuevo tipo de herramientas de ataque llamadas en un principio *caballos de Troya* y más tarde, por economía del lenguaje, tan solo troyanos. El nombre es una analogía con lo narrado por Homero en *La Odisea* y por Virgilio en *La Eneida*. En esas obras clásicas se explica que el ejército griego, ante la imposibilidad de tomar la ciudad amurallada de Troya, construyó como supuesto homenaje a sus defensores un gigantesco equino de madera. Estos lo introdujeron sin saber que en su interior se escondían soldados que, al anochecer, mataron a los centinelas y abrieron las puertas. Los asediadores entraron y la plaza fue conquistada a sangre y fuego. En el mundo de la informática no hay muertes, pero permanece la idea de meter a un pequeño enemigo en las tripas del ordenador para controlarlo a voluntad por alguien de fuera.

En algunas ocasiones la *intrusión* no es tal, puesto que está aceptada por ambas partes. Son las aplicaciones de control remoto como Teamviewer, del que hablamos en el capítulo cinco cuando lo empleó *MrBank* para robar millones de números de tarjetas bancarias en España. El servicio técnico de muchas empresas y, cada vez más, de particulares, instala el programa en los ordenadores que deben monitorizar. Cuando el usuario tiene un problema, el operador ejecuta su herramienta y consigue visualizar el monitor de la otra parte como si fuera el suyo propio. De esta forma es mucho más fácil encontrar lo que no funciona que mediante una conversación telefónica en la que muchas veces el ciudadano medio no tiene los suficientes conocimientos para explicarse o seguir las indicaciones del experto. Estos programas sortean antivirus y cortafuegos porque ha ido una persona al domicilio y lo ha instalado, deshabilitando, si hubiera sido necesario, los sistemas de seguridad. Una vez hecho, funciona a través de ellos, salvo que el dueño del equipo decida comprobar a mano los permisos concedidos, algo que muy pocas personas hacen. *MrBank*, al ser un trabajador contratado, tenía acceso total a las terminales bancarias, lo que aprovechó para dejar su pequeño regalito con el que podía luego acceder desde su domicilio. Además, tomó ventaja del hecho de que estaban muy en el interior del sistema, donde no había de manera continua un operador delante del teclado, porque Teamviewer no está pensado para pasar desapercibido, sino que avisa cuando está activo. Cualquiera repararía en que hay un icono extraño en la parte inferior de la pantalla.

Para controlar el ordenador, tableta o teléfono móvil de otra persona no hace falta ni siquiera saber programación. En los foros del mundo *hacker*, cada vez más a menudo situados dentro de las redes anónimas como TOR, es posible descargar herramientas listas para hacerlo. Eso sí, quien lo busca se arriesga a que le salga el tiro por la culata. Nada le gusta más a la comunidad de la seguridad informática que hacer morder el polvo a quien llaman *lammer*, alguien que quiere aparentar saber

mucho pero en realidad es un ignorante. Es, por tanto, posible que lo que ha obtenido sirva para infectar su PC tanto como él quería acceder al de su víctima y que no se dé cuenta de ello nunca.

De una manera u otra, cuando el criminal consiga las dos partes que componen su troyano, la de infección y la de manejo, lo único que ha de hacer es engañar a su víctima para que instale la primera. Puede hacerlo de muchas formas. Las más habituales son haciéndole creer que ha recibido un correo electrónico con un archivo adjunto que simula ser una fotografía, una postal electrónica, una factura, etc. El límite está en la imaginación de cada cual. Cuando el objetivo intenta visualizarlo y hace doble clic en el mismo, se ejecutan las líneas de código malicioso y se produce la infección. Desde ese momento el atacante ya tiene el control sobre el aparato de su víctima. Lo que sea o no capaz de hacer depende de su habilidad programando o de la aplicación que esté usando. Una de las más célebres y fáciles de usar, llamada *Poison Ivy* —Hiedra Venenosa en inglés— da un dominio casi absoluto del ordenador objetivo. La parte destinada a infectar al objetivo es muy pequeña, de menos de diez *kilobytes* —fácil, por tanto, de hacer llegar a través de Internet— y se copia en la propia carpeta Windows, con lo que queda escondida y es difícil de eliminar incluso si es detectada. El atacante elige lo que quiere hacer en un sencillo interfaz gráfico, utilizable por cualquiera incluso con conocimientos de informática muy escasos, y permite desde *nimiedades* como abrir y cerrar el lector de DVD a voluntad a la captura de todas las contraseñas que se tecleen, activar la cámara web sin que haya ningún indicio externo que lo muestre o abrir y cerrar ventanas del sistema operativo. Su código fuente es libre y público, por lo que cualquiera con la debida formación puede reescribirlo a placer para dificultar su detección o añadirle nuevas características. Incluso en la Internet abierta es fácil encontrar versiones de *Poison Ivy* y manuales para su uso, como en *Programas-hack.com*, por ejemplo. Nada garantiza que *ese* programa que nos hemos descargado no tenga a su vez un *bicho* dentro que nos ponga en manos de algún otro malintencionado, en especial porque uno de los requerimientos de todos estos troyanos para instalarse y funcionar es desactivar el antivirus.

En el año 2007, la Brigada de Investigación Tecnológica de la Policía Nacional llevó a cabo una operación llamada Hydra contra la descarga de pornografía infantil en Internet. Entre los detenidos, destacó un individuo residente en la provincia de Burgos. Cuando los agentes de la Brigada Provincial de Policía Judicial, que colaboraban con la BIT, realizaron el registro de su domicilio, encontraron, además de las imágenes de menores, que era un avezado usuario de ese tipo de programas-espía. En el posterior estudio de su material se detectaron cientos de intentos de ataque a través de uno de esos troyanos preconfigurados, siempre orientados a niñas que conocía en salas de chat y a las que camelaba para conseguir su dirección de correo electrónico para continuar el contacto. Solo con el cinco por ciento había tenido éxito, aquellas que no tenían un antivirus instalado. Se centraba en buscar

documentos privados en el ordenador y en realizar fotografías a través de la cámara web cuando las pequeñas se cambiaban de ropa o se iban al baño. En una ocasión descubrió que la persona con la que hablaba no era la menor que aparentaba ser, sino un adulto que se hacía pasar por tal para, como él, engañar a otros chavales. Guardó todo lo que obtuvo de él, incluyendo currículos personales donde salía su nombre y puesto de trabajo —en un colegio de la localidad gerundense de Figueras— en una carpeta con el nombre «Profe malo», como luego encontraron los agentes que realizaron el informe pericial.

Usaba la misma técnica el conocido como *Hacker de las actrices*, entre cuyas víctimas estaba Hiba Abouk, famosa por su papel en la serie de Telecinco *El príncipe*. Una vez que conocía el correo electrónico de una celebridad, le enviaba un mensaje en el que simulaba que había realizado una compra que debía aceptar o cancelar. Por supuesto, era mentira y la página a la que accedían estaba diseñada por él y solicitaba, simulando un acceso legítimo, el nombre de usuario y contraseña del correo electrónico, como si hubiera habido una desconexión y tuviera que identificarse de nuevo. Desde ese momento, lo podía controlar y lo usaba para enviar troyanos a terceros que pensaban de buena fe que su interlocutora era la original y no su suplantador. Así tenía acceso a sus terminales y a todo lo que tuvieran guardado en la nube. Tenía antecedentes por hechos similares en 2014 y 2015, entonces con personajes del mundo de la moda, lo que le había hecho tomar medidas de precaución pensando que escaparía al rastreo de los agentes. Craso error. Fue detenido por la BIT en Córdoba en marzo de 2016.

Todos los equipos domésticos son susceptibles de ser atacados con éxito. Solo es necesario que un verdadero *hacker* tenga el suficiente empeño. Las grandes empresas tienen equipos de especialistas dedicados solo a descubrir y bloquear intentos de intrusión —y aun así se las cuelan—, pero nosotros, simples mortales, solo podemos confiar en no llamar demasiado la atención. Incluso si somos precavidos a la hora de no aceptar documentos extraños que lleguen por correo electrónico, podemos ser víctimas de algún error de programación.

Los teléfonos móviles inteligentes, que están sustituyendo a los ordenadores como máquina preferida para acceder a Internet, tienen unos sistemas operativos que requieren técnicas diferentes a los PC domésticos. No es suficiente que la víctima pulse el adjunto de un correo, sino que hay que convencerla para que instale la aplicación maliciosa que, por supuesto, no está en las tiendas oficiales —la Play Store para Android y la App Store para iPhone—, que tienen una supervisión continua por parte de los responsables de Google y Apple. Además, la mayoría de terminales vienen protegidos contra ese tipo de instalaciones *de origen desconocido*, por lo que hay que modificar los ajustes a mano y luego instalar el programa malicioso. Tal vez porque confía en el remitente, quizá porque su teléfono ya estaba desprotegido, siempre hay alguien que es engañado. Cuando la víctima le ha dado acceso al atacante, este puede obtener contraseñas para controlar los correos electrónicos y

cuentas de almacenamiento en la nube, por lo que se puede descargar fotografías íntimas allí almacenadas o suplantarla enviando correos a su lista de contactos que, al provenir de su propia cuenta, pueden crear engaño suficiente y hacer que otros amigos piquen y extender de esta manera la infección.

Hay una forma de obtener datos de terceros que no requiere infiltrar ningún *bicho* en el ordenador del objetivo. Basta estar presente en la misma red para tener acceso a mucho más de lo que a un lego le parece posible. Hasta hace unos años, la única forma de lograrlo era con un cable enchufado al *router* que se quería infiltrar. Hoy resulta mucho más fácil en un mundo lleno de conexiones inalámbricas. La seguridad actual de estas redes es suficiente en la mayoría de los casos si su administrador se ha molestado en configurarla bien. El primer error que suele cometer un usuario medio es no cambiar la contraseña que viene de origen. Estas están relacionadas con el nombre por defecto de la red —que también hay que cambiar— como Orange-39E8 o Vodafone9D67. Cualquiera puede usar un programa para, sabiendo cómo se llama, descubrir su clave. Una vez que un intruso está dentro puede espiar todo lo que hay en el interior. Para hacerlo, utiliza un *software* conocido como *sniffer*, porque «huele» todo lo que pasa por su camino. Recordemos del capítulo uno que la información en Internet se mueve por paquetes de datos y estos en primer lugar van del ordenador a la red para de ahí llegar al *router* y, de este, a Internet. El *sniffer* hace una copia de todos y cada uno de los paquetes, aunque no vayan destinados al ordenador que lo tiene instalado, y luego va reconstruyendo la información. Así puede obtener contraseñas, por ejemplo, o hábitos de navegación, correos electrónicos y muchas más cosas. Una *WiFi* desprotegida, que permite un acceso sin necesidad de registrarse, puede ser una trampa para un incauto que quiera usar sus servicios cuando, en realidad, quien la ha configurado está espiando el tráfico del intruso.

Puede ser todavía peor. La mayoría de los hogares tienen configuradas sus redes como «domésticas» o «de confianza». Eso quiere decir que los dispositivos que están dentro de ella tienen una serie de privilegios entre sí de los que no dispone quien está fuera. Por ejemplo, puede acceder a las impresoras o incluso a los discos duros, según la configuración. Un intruso, por tanto, puede robar fotos, archivos personales —mucha gente tiene una copia escaneada de su DNI o de sus claves bancarias— o colocar un troyano. Solo tendrá que esperar a que el legítimo dueño lo active para conseguir lo que hemos visto más arriba, incluido activar la cámara web. Esto es lo que hacía un vecino de Zaragoza de treinta y cuatro años que fue detenido el 6 de noviembre de 2012. Aprovechaba sus conocimientos informáticos para espiar a más de cien personas, todas aquellas cuyas redes inalámbricas tenía a su alcance y que no habían cambiado la contraseña o tenían una seguridad anticuada. Había obtenido cientos de fotos, capturadas a intervalos de tres segundos, de sus vecinas, en especial cuando se desnudaban o mantenían relaciones sexuales. Su error fue que, además, se descargaba pornografía infantil que, como hemos visto, es uno de los delitos más perseguidos. Al llegar al domicilio, los agentes de la Policía Nacional en Zaragoza

descubrieron lo demás.

APROVECHAR LA VULNERABILIDAD PARA CONSEGUIR UN BENEFICIO

Si un *hacker* quiere entrar en nuestro ordenador es casi seguro que lo va a hacer. Por suerte, la mayoría de nosotros no somos apetecibles para ellos. Además de con engaños o con nuestra involuntaria colaboración, un experto dedicado puede recurrir a muchos elementos que pasan desapercibidos al común de los mortales. Los sistemas operativos y los programas que utilizamos a diario tienen una complejidad asombrosa. Además, para garantizar la compatibilidad con modelos anteriores llevan una historia de adaptaciones de código antiguo detrás, parche sobre parche, corrección sobre corrección. Eso significa que es muy fácil que existan agujeros, vulnerabilidades no descubiertas, como las que ya vimos en el capítulo tres al hablar del virus *Stuxnet* que atacó las centrales nucleares iraníes. En cuanto alguien da con ellas, los fabricantes se afanan en solucionarlas lo antes posible. El problema está en aquellas que ha encontrado un experto malintencionado y no tiene ninguna intención de comunicar, sino que prefiere usarla para sus aviesos propósitos. Aquí encontramos una diferencia fundamental entre *hackers*. Mientras los hay que están dispuestos a hacer dinero rápido a costa del ajeno, incluyendo ponerse al servicio de las mafias africanas o del Este de Europa, la mayoría se dedican a intentar intrusiones por *hobby* o hasta como salida laboral. Prueban la seguridad de un sistema, programa o sociedad y comunican los fallos que han encontrado. En España hay verdaderos expertos reconocidos a nivel mundial, como Chema Alonso, inconfundible siempre con su gorro de lana y su melena suelta debajo. Es autor del imprescindible blog *Un informático en el lado del mal*. En 2012 Telefónica le contrató junto a todo el personal de su empresa, Informática64, para mejorar la ciberseguridad y en 2016 fue ascendido a jefe de toda el área. Otro reconocido especialista es Lorenzo Martínez, uno de los fundadores del blog Security By Default, ahora a cargo de su propia compañía, Securízame, dedicada a consultoría, auditoría y formación específica en seguridad. Es un profesional multidisciplinar, pero, por lo que me ha contado, lo que más le gusta es el análisis y peritaje forense. De hecho, ha participado en el esclarecimiento de varios *crímenes digitales* y ha ayudado a empresas que, por no haber invertido en seguridad desde el principio, han terminado pagando las consecuencias, en muchos casos, en Bitcoins. Dejando a un lado a profesionales como los mencionados, otros, que *trabajan* por libre, haciendo *auditorías* —ataques— que nadie ha pedido, pueden encontrar que su objetivo puede interpretar sus intenciones como maliciosas y no dudar en denunciarle y lograr su condena. Después de todo, ha cometido un delito tipificado —en el código penal español, por ejemplo, como *daños informáticos*— y suele haber causado un perjuicio grave.

Los *hackers* delincuentes requieren un beneficio más rápido del que se puede

llevar a cabo al invadir ordenadores de uno en uno. Por ello, una vez detectada una vulnerabilidad en cualquier programa, idean una herramienta que les pueda servir para sus propósitos, de una complejidad muy variable. Algunos de ellos no difieren demasiado del *phishing* que vimos en el capítulo seis. En 2012 la empresa de seguridad Eset detectó un código malicioso en hasta veintidós aplicaciones Android, llamado *Boxer*, que infectaba el teléfono y suscribía a sus víctimas, sin que ellas lo detectasen, a un servicio SMS *Premium*. Este tipo de mensajes telefónicos tienen la característica de que la empresa emisora cobra a quien los recibe; es el receptor quien paga por ellos. Aunque su uso es legal —por ejemplo para obtener consultas de astrología solicitadas de antemano—, es utilizado con asiduidad por los delincuentes. *Boxer* era capaz de detectar el país en que se encontraba y redirigir los SMS a una u otra empresa. En España el número en cuestión era el 35969, de la empresa World Premium Rates, cuyo principal contratista legal era un número de tarot de Tenerife. Como los teléfonos Android no pueden infectarse sin la colaboración activa de su dueño, el *gancho* que utilizaban era el de aplicaciones con apariencia de juegos o sobre salud que el incauto instalaba sin saber que, desde ese momento, cada vez que la ejecutaba, hacía que le enviasen tres SMS de alto coste, engordando de manera notable la factura a fin de mes.

Dos años después, el antivirus español Panda Security avisaba de cuatro aplicaciones que se habían colado durante un tiempo en la tienda de Google —hasta que fueron detectadas y eliminadas— con una forma de funcionamiento muy similar, aunque todavía un poco más intrincada. Sus nombres eran «Dietas para reducir abdomen» y «Peinados Fáciles» de Clark Beggage por un lado y «Cupcakes recetas» y «Rutinas y ejercicios para el *gym*» de CanarApp por otro. Una vez instalada, mostraba un aviso en segundo plano y tamaño ilegible sobre lo que nos iban a cobrar por el mero hecho de usarla, para darle una apariencia de legalidad que, de hecho, no tenía. A partir de ahí, la programación era más sofisticada que los anteriores. Los servicios SMS *Premium*, para evitar estos abusos, exigen introducir un código de seguridad que envían al usuario, también mediante mensaje de texto. Pues bien, este virus capturaba el número de teléfono del usuario —que, por diseño de los terminales, suele ser invisible para las aplicaciones—, que es obligatorio proporcionar para acceder a la mensajería instantánea de WhatsApp. Una vez que lo tenía, se suscribía al servicio y, sin que el usuario lo viese, recibía el mensaje de confirmación y validaba el código. Después eliminaba los SMS recibidos y enviados. De esta forma, hasta la primera factura la víctima no era consciente de que estaba infectada.

El año anterior, la Brigada de Investigación Tecnológica de la Policía Nacional detuvo a un ingeniero murciano de veintitrés años que había estafado, en tan solo dos meses, a más de once mil personas, lo que le proporcionó un beneficio de cuarenta mil euros, gracias en parte a una intensa campaña de publicidad *online*. Usaba uno de los ganchos más populares entre aquellos con menos cultura informática: WhatsApp

Spy, un programa que prometía espiar las conversaciones a través del servicio de mensajería instantánea de aquel usuario que se desease. Eso, de ser cierto, constituiría un delito grave, descubrimiento y revelación de secretos, dado que la privacidad de las comunicaciones está garantizada en la Constitución. Pero no lo hacía. Era tan solo una simple estafa, mucho más fácil de programar que las dos vistas en párrafos anteriores. Tan solo era una página web en la que los incautos proporcionaban su número telefónico y empezaban a recibir mensajes que llegaban a costarles algo más de siete euros en algunas ocasiones. Además, había creado otro sitio que simulaba la presentación de Facebook. Los incautos que querían comprar su aplicación volvían a ingresar sus datos pensando que, por algún motivo, habían sido desconectados. En realidad, los datos aportados quedaban almacenados en un servidor externo del que sus programas los cogían para hacerse pasar por aquellos usuarios y enviar mensajes masivos a todos sus contactos hablando de las bondades del inexistente programa espía.

La forma de actuar no es nueva. En la primera década de este siglo eran muchos los timadores que, anunciándose a sí mismos como *hackers*, prometían averiguar las contraseñas de los programas de mensajería instantánea, como el que entonces triunfaba, MSN Messenger. Para ello solo exigían que el que quería obtener esa información les enviase un correo con su propia contraseña. A cambio, prometían dar las de su objetivo. El truco era tan burdo que sorprendía la cantidad de incautos que caían. Por supuesto, lo único que conseguían aquellos era perder su cuenta de correo, que pasaba a manos del embaucador.

Tampoco los usuarios de Apple están más a salvo. A finales de 2015 se descubrió que durante meses, decenas de aplicaciones presentes en la App Store, en la que los poseedores de un iPhone deben descargar los programas que quieren utilizar, habían sido programadas con una versión pirata de XCode, el lenguaje en que se escriben. Esta, apodada XCodeGhost, envía datos muy relevantes de aquellos que se la bajaban, como su identificador único o IP de acceso. El motivo de un agujero de seguridad tan grande es tan trivial como absurdo. Algunas grandes empresas chinas se descargaban XCode de una web llamada *Baidu Pan*, muy popular en China y parecida a otros servicios de almacenamiento en la nube a los que estamos más acostumbrados en España, como Dropbox, donde alguien había reemplazado la original por la maliciosa. Podían bajarse el lenguaje de programación del propio sitio de Apple, pero sus servidores eran más lentos. Así, la versión maligna fue utilizada por decenas de programadores causando un daño cuyo coste todavía se está analizando.

Las vulnerabilidades lo son hasta que alguien las empieza a usar de esta forma masiva. En ese momento no tardan en ser descubiertas por las empresas de seguridad, que comienzan a diseñar soluciones lo antes posible. Por eso, un antivirus actualizado y un cortafuegos que bloquee las señales entrantes y salientes no autorizadas es efectivo en un porcentaje que se acerca a la totalidad, puesto que no es el empeño de

un particular en conseguir la intrusión, sino una manera de conseguir datos o dinero de forma automatizada. Estos son los ataques más habituales de los que todos somos víctimas. De hecho, el empeño de un *hacker* en nosotros, pobres mortales, es la excepción. La mayoría de usuarios jamás se enfrentará a uno. Por si esa necesidad fuera poca, a cualquier ataque no tardan en salirle imitadores buscando aprovecharse de la idea para robar que otro ha tenido. Hay poco honor entre ladrones.

Existe una clase de amenaza cibernética más dañina, que en la actualidad tiene miles de *clones* con comportamientos muy parecidos. Por su forma de operar se clasifica entre los troyanos, es decir, aquellos que toman el control de un ordenador. Dentro de estos, se denomina *ransomware*, que se puede traducir como «programa que pide un rescate». Su comportamiento es muy perjudicial y en cada nueva versión lo es más todavía. Una vez infectada la máquina objetivo, evita que se pueda usar con normalidad salvo que se pague una multa en Bitcoins o mediante plataformas de pago poco rastreables, como uKash.

En 1989 se tuvo conocimiento del primero de estos troyanos, conocido como AIDS, el acrónimo en inglés de sida. Estaba programado por el estadounidense Joseph Popp. La evolución de estos programas se hizo bastante popular en Rusia en la primera década de este siglo. En Europa Occidental nos mantuvimos bastante ignorantes hasta el año 2011, con la llegada del Virus de la Policía. Tenía un funcionamiento tan sencillo como eficaz. Al visitar una página web poco segura —como de descarga de contenidos de derechos de autor o algunas pornográficas— se ejecutan multitud de pequeños programitas escritos en el lenguaje Java, el más habitual en Internet. Su función, en condiciones normales, es de publicidad; mostrar anuncios en ventanas flotantes o ejecutar pequeños vídeos. Entre todos estos se encuentra nuestro amigo, que la empresa de seguridad Kaspersky llamó *Trojan.Ransom* —Troyano.Rescate—. Aprovechaba un pequeño error del cliente de Java que todos tenemos en nuestros ordenadores que le permitía *colar* el bicho. Una vez que se instalaba, mostraba una muy alarmante pantalla: nuestro equipo estaba bloqueado por haber descargado pornografía infantil o películas protegidas por derechos de autor. Más adelante incluyó otros delitos, como apología del terrorismo. Utilizaba fotografías de operaciones de la Policía Nacional y hasta sus logotipos para hacer la estafa más creíble. En un lugar prominente mostraba instrucciones para pagar una multa de cien euros con tarjetas uKash o Paysafecard y así terminar con el *secuestro*. Incluso explicaban dónde se podían adquirir las tarjetas que debían usarse. Hasta que no se pagase, lo único que mostraba el equipo era la pantalla del virus. No se podía utilizar ningún documento ni aplicación.

Aquel marzo apareció por primera vez, con un mensaje que fingía ser de la policía alemana. En junio se expandió por los países más importantes de la Unión, incluida España, y la Policía Nacional emitió un primer aviso a la ciudadanía para que no picara. Según la dirección IP del que resultaba infectado se mostraba una pantalla diferente, de forma que cada internauta veía un mensaje de quien afirmaba

ser una agencia legal de su propio país.

Tan pronto como los desarrolladores de Java se dieron cuenta, corrigieron el problema y ya no pudo funcionar en ordenadores actualizados. También los antivirus hicieron su trabajo y, tras unos meses, su eficacia fue mínima. Hasta entonces, las comisarías y los correos de atención al ciudadano de la Brigada de Investigación Tecnológica recibían cientos de avisos de ciudadanos que pedían ayuda porque ellos no habían hecho nada ilegal. Muchos pagaron sin que el ordenador quedase liberado —dado que el virus no estaba escrito para destruirse o retirar su actividad—. Algunos, al ver que con el primer envío de dinero no lo recuperaban, compraron dos y hasta tres tarjetas. A pesar de que según estimaciones de la OSI, Oficina de Seguridad del Internauta —organismo que forma parte del Instituto Nacional de Ciberseguridad, dependiente del Ministerio de Industria—, los que usaron un medio de pago no fueron más que el ocho por ciento de los infectados, el beneficio para los autores fue inconmensurable, por lo que no tardaron en salirles imitadores.

En enero de 2012 se multiplicó el problema, con decenas de miles de usuarios afectados en todo el mundo, con multitud de versiones diferentes. A partir del mes siguiente comenzaron a utilizar una nueva vulnerabilidad en Java, por lo que de nuevo hasta aquellos que estaban actualizados corrieron riesgos. Para entonces, la OSI ya había publicado una herramienta de desinfección y una serie de instrucciones para que los usuarios que lo sufrían pudieran recuperar su uso.

Lo peor aún estaba por venir. Desde abril, los virus cifraban los archivos de trabajo, como los de Word, Excel, fotografías y PDF. Esto significaba que incluso si se eliminaba al atacante, los documentos quedaban inservibles. Eso puede ser un pequeño drama en una familia y una auténtica catástrofe en una empresa. Por fortuna, todavía no eran demasiado complejos y las empresas de seguridad Dr. Web y Kaspersky desarrollaron programas gratuitos para solucionarlo. Para hacerlo era necesario disponer de una copia sana en un dispositivo externo como un USB de al menos uno de los archivos que habían sido cifrados. Comparando la versión cifrada con la original, eran capaces de calcular la clave y de esta forma liberar todo el disco duro. Oracle, propietaria de Java, publicó en mayo la versión 7 de su programa, que solucionaba por fin y sin necesidad de parches el problema. Solo faltaba que la gente se actualizara… y algunos usuarios son muy reacios, bien por vagancia, bien por no tener suficientes conocimientos informáticos.

Las variantes continuaron su adaptación al trabajo que se llevaba a cabo para contrarrestarlas. Algunas activaban la cámara web del sujeto, con la consiguiente alarma al creerse espiado todo el tiempo. En realidad, las fotos no se enviaban a ningún sitio —hubiera sido un riesgo para la seguridad de la banda criminal—, sino que tan solo se mostraban a su dueño para asustarle. Al mismo tiempo, alteraban el ordenador para no poder acceder a los recursos de recuperación que incluía el propio sistema operativo. Hasta aparecieron ataques para Macintosh, los ordenadores de la casa Apple, que tienen una falsa reputación de no tener amenazas que les afecten.

Otras versiones incluían fotografías de abusos a niños como si hubieran sido descargadas por el propio usuario o accedía al historial de navegación para usarlo en su contra.

Mientras tanto, la Policía Nacional no estaba de brazos cruzados. El Grupo de Seguridad Lógica de la Brigada de Investigación Tecnológica, con la ayuda de Europol, ya llevaba un agotador año detrás del responsable. Utilizaron una combinación de técnicas informáticas y tradicionales, que incluían agentes encubiertos, acceso desde una prisión a foros de *hackers*, intervenciones telefónicas y vigilancias, así como rastreo del movimiento del dinero. Encontraron a alguien que se hacía llamar *Limbo* y *Abramovich* y que parecía estar muy arriba en la organización. Sin demasiada sorpresa para los investigadores, resultaron ser la misma persona, el ruso Alexander Krasnokutsky, de veintisiete años, programador y jefe de la banda que no paraba de introducir mejoras en su criatura. En ese momento había ya cuarenta y ocho clones diferentes del virus.

A medida que la investigación avanzaba, los agentes detectaron a otros diez individuos trabajando para él, desarrollando nuevas adaptaciones, recibiendo los pagos fraudulentos y blanqueándolos, para lo que utilizaban *mulas*, como ya explicamos en el capítulo seis. Una vez que se tuvo la seguridad de que toda la red estaba localizada, decenas de agentes se desplazaron a la provincia de Málaga para detenerlos y desmantelarla. Justo antes del operativo descubrieron, con gran frustración, que *Limbo* no estaba ya allí. ¿Había huido? ¿Podía haber un topo que le hubiera dado el aviso desde dentro? ¿O había detectado las vigilancias, electrónicas o físicas, y había emigrado, dejando tirados a sus secuaces? Se habló con el juzgado que llevaba el sumario, el Central de Instrucción número 3 de la Audiencia Nacional, para retrasar unos días el operativo. Fueron jornadas de trabajo frenético, desde Madrid y Málaga al mismo tiempo, para lograr ubicarlo. Si escapaba, no tardaría en encontrar otro grupo de secuaces y seguir delinquiendo. Pronto supieron que había salido de España. Eso dificultaba más la tarea. El mundo es un lugar muy grande. Sin embargo, no estaba asustado y se puso en contacto con su banda… desde Dubái, en los Emiratos Árabes Unidos. Había ido a pasar las Navidades allá. Dos agentes de la BIT acudieron de inmediato a vigilarlo, con la dificultad añadida de pasar desapercibidos en un país tan diferente al suyo propio. El magistrado Javier Gómez Bermúdez dictó una orden internacional de detención que las autoridades de aquel país ejecutaron con la debida diligencia a comienzos de 2013. No tardaría en ser extraditado a España.

Solo después de tener asegurado a Krasnokutsky se desató el operativo en Benalmádena, donde fueron arrestados ocho miembros de la banda, y Torremolinos, donde cayeron otros dos. En total, seis rusos, dos ucranianos y dos georgianos. Blanqueaban un millón de euros al año, todos procedentes de los incautos que pagaban las falsas multas. Muy lejos de las poco más de novecientas denuncias —de los que menos de la mitad reconocían haber pagado— y más cercanas a las casi

ochocientas mil consultas que había recibido la OSI. Por vergüenza o por la poca cantidad defraudada, gran cantidad de víctimas no habían informado de lo ocurrido a la policía.

En septiembre de aquel mismo año, fruto del estudio del material intervenido, cayeron otros dos colaboradores, ucranianos y residentes en Madrid. Eran una *subcontrata*, es decir, otra empresa criminal que tenía como clientes a otros delincuentes. Para la banda de *Limbo* proporcionaban servicio de alojamiento a los servidores desde los que se enviaba la estafa, como uno de los más famosos, *www.lapoliciaespanola.org*. Pero había más. La investigación a la que fueron sometidos antes de su detención mostró que estaban blanqueando dinero, hasta diez mil euros diarios, para lo que usaban un hábil sistema de transferencias y compraventa de monedas virtuales, entre las que destacaban las Bitcoins y dólares Linden, ambas explicadas en el capítulo anterior. Cuando los atraparon, habían blanqueado al menos seiscientos mil euros provenientes de sus delitos. En sus domicilios encontraron, en efectivo, cincuenta y cinco mil euros, entre moneda real y monederos virtuales. De esta manera, la Policía Nacional de España se convirtió en el segundo cuerpo mundial, después de la DEA estadounidense, en aprehender Bitcoins.

No acababan ahí sus *logros*. Habían conseguido infiltrarse en hasta veintiuna mil empresas de ochenta países —mil quinientas de ellas en España—, todas ellas con servicios de escritorio remoto mal configurados, sin las adecuadas medidas de protección. Después vendían el acceso a los servidores de esas empresas, al módico precio de diez euros cada uno. Otros delincuentes los utilizaban después para sus aviesos propósitos. Durante aquellos días de 2013 fue habitual encontrar, en directorios ocultos para sus legítimos dueños, páginas donde se ofrecía la venta de pornografía infantil. A medida que eran descubiertos, la policía los eliminaba y estudiaba los accesos. Todos ellos llevaban a *proxies* muy difíciles de rastrear, el típico *modus operandi* de los grupos organizados.

En febrero de 2016 se celebró el juicio en la Sala de lo Penal de la Audiencia Nacional. Justo antes de su inicio, los acusados llegaron a un acuerdo con el fiscal. A cambio de aceptar todos los cargos que les imputaban, consiguieron una notable rebaja en su estancia entre rejas. Los dieciocho años de prisión que se pedían a Krasnokutsky se quedaron en seis. El resto de la banda salió mejor parado aún, entre tres meses y tres años de reclusión, de los que la mayoría no cumpliría ni un día. La delincuencia financiera —no así otras— sale muy barata en España.

Cuando el grupo de *Limbo* dejó de actuar, una multitud de imitadores explotó el filón. Después de todo, era una manera fácil de hacer dinero, sobre todo si se tomaban precauciones adicionales. Algunas copias, una vez solventados los problemas con Java, lo único que lograban hacer era bloquear la pantalla del navegador. Bastaba cerrarlo para que todo volviese a la normalidad. Otros se centraron en Android, pero, como ya hemos visto, los teléfonos no son tan vulnerables como un ordenador. De nuevo había que convencer al incauto de que

descargase e instalase una aplicación por propia voluntad. Aun así, el bloqueo que hacía no era irreparable.

El peor de esta familia apareció a finales de 2013, aunque se identificó por las autoridades en mayo del año siguiente. Se conoce como *Cryptolocker*, esto es, «que bloquea mediante criptografía» y el FBI sospecha que fue creado por el ruso Evgeniy Mikhailovich Bogachev, alias *Lucky12345*, *Slavik* y *Pollingsoon*. La agencia estadounidense ofrece en su página sobre los más buscados a nivel mundial hasta tres millones dólares por cualquier pista que lleve a su detención. Está acusado de una multitud de delitos económicos, que incluyen otro *malware*, con el que accedía a contraseñas bancarias que desvalijaba en todo el mundo. La cantidad robada se estima en al menos cien millones de dólares.

El funcionamiento de *Cryptolocker* es más complejo que los anteriores. La infección ocurre de la forma tradicional, al abrir un adjunto de un correo electrónico —de nuevo un comportamiento que cuenta con la colaboración de la víctima, engañada— o bien porque el equipo ya tiene otras amenazas instaladas —como un troyano llamado *Zeus*, también diseñado por Bogachev— que permiten a los delincuentes acceder y colocar el nuevo *bichito*. En cualquier caso, ya no es posible la instalación inadvertida del mismo, como pasaba con los errores de Java. Una vez en el ordenador se dedica a cifrar, como su antecesor, los archivos de trabajo (Word, Excel, etc.) pero, en vez de mantener la clave para su solución en el equipo, lo que permitía que los antivirus publicaran utilidades para recuperarlos, lo guarda en un servidor remoto. Además, utiliza encriptado asimétrico —recordemos el capítulo anterior— y de una complejidad tan poderosa que, sin la clave privada y con la potencia de computación actual, podrían pasar miles de años antes de resolverlos. El agraviado debía pagar una cantidad equivalente a trescientos cincuenta dólares en Bitcoins o el servidor destruiría la clave privada. Muchos lo hicieron, sobre todo empresas a las que perder sus bases de datos podía resultar mucho peor. Algunos expertos en seguridad admitieron que era la única forma de volver a la normalidad, una vez eliminado el troyano en sí mismo, algo sencillo. El 2 de junio de 2014, como parte de la Operación Tovar de Interpol, varias universidades y empresas privadas de seguridad informática atacaron y desmantelaron los servidores, que eran parte de una *botnet* —concepto que veremos a continuación— y en Holanda se recuperó una ingente cantidad de claves privadas con las que las empresas Fox-It y FireEye desarrollaron un programa gratuito mediante el que los afectados podían subir un archivo cifrado y con un poco de suerte, conseguir la solución.

Hoy sigue habiendo nuevas versiones, aunque parecen no estar relacionadas con la original. Las más recientes guardan las claves privadas en servidores de la red TOR, más difíciles de encontrar. El creador de uno de estos virus, que se hace llamar *Whiterocks*, los ha puesto a la venta, de manera que cualquiera puede montar su propia red de secuestro de ordenadores. Ha establecido dos modelos, cuatrocientos dólares si solo se quiere el *bichito* y su forma de operarlo, y tres mil si lo que se desea

es el propio código, es decir, cómo ha sido programado, lo que permite estudiarlo para introducirle mejoras. El anuncio se puede encontrar con facilidad en la web Pastebin.

LAS HORDAS DE ORDENADORES ZOMBIS

Hay maneras de que nos cuelen un virus que tome el control de nuestro ordenador sin que ningún antivirus lo pueda detectar, de una forma muy parecida a lo que pasó en la Apple App Store, debido al *software* pirata. En nuestro país, todavía hoy es habitual que los sistemas operativos de muchos ordenadores domésticos se hayan descargado de Internet sin unas mínimas condiciones de seguridad. Se accede a ellos en páginas de descarga directa o en programas P2P como eMule. Nadie se pregunta quién lo ha colgado ni qué han tenido que hacer para retirar las protecciones de seguridad. Ya hemos visto en el transcurso de este libro que el altruismo en Internet es algo muy escaso, menos aún desde que su vertiente económica cobró tanta importancia. Aunque la persona que ponga un Windows pirata en las redes lo haga sin intereses ocultos, quien se lo pasó, el sitio del que lo obtuvo, posiblemente metiera un troyano en las tripas más profundas. Romper la seguridad de un *software* tan sofisticado es muy costoso y difícil. Hacen falta conocimientos y esfuerzo. Es esperable que se intente obtener un beneficio de ello.

Un *bichito* metido dentro de aquello que hace que el ordenador arranque, que controla sus más básicas funciones y hace que las demás trabajen, tiene una ventaja fundamental respecto a los que actúan de forma más superficial, que los antivirus no lo van a detectar. Está fuera de su alcance. Así, pueden asegurarse un rendimiento casi indetectable.

Otra fuente de infección menos agresiva la constituyen el resto de programas pirateados y sus *cracks*, o sea las aplicaciones que sirven para romper su seguridad y poder usarlos como si fueran legítimos. Estos, a menudo, piden que se desactive el antivirus como paso previo a su instalación. Es tan arriesgado como suena. En cualquier caso, instalar cualquier tipo de programa que ha sido manipulado por terceros es peligroso.

Estas *enfermedades* suelen ser masivas. Son programas al alcance en Internet de cualquiera que no pueda o no quiera rascarse el bolsillo y lo mejor de todo es que funcionan a pesar de su contenido extra. Otros tipos de troyanos ocultos en engaños como falsas fotografías o archivos de Acrobat Reader (los famosos PDF) son más sencillos de detectar porque no cumplen lo que se supone que deben hacer, mientras que quien se instala un Windows 10 pirata sí que consigue que su ordenador opere con él a las mil maravillas. Lo que no sabe, ni aunque tenga el mejor de los antivirus, es que ha entrado a formar parte de lo que se conoce como *botnet*, esto es, un conjunto de ordenadores bajo el control de una persona u organización sin que sus

legítimos propietarios sean conscientes de ello. No le roban sus contraseñas bancarias, no hacen que se conecte la cámara web, no le cifran sus archivos… En apariencia, nada ocurre, por lo que desconoce que su equipo es un zombi al servicio de un desconocido. Se calcula que hay al menos cien millones de PC en todo el mundo que forman parte de alguna *botnet*.

Estas permiten a un criminal realizar operaciones que no podría llevar a cabo solo con una conexión o con un pequeño grupo de ellas. Puede habilitar los ordenadores de las víctimas como una suerte de servicio de *proxies*, utilizando las conexiones a Internet de aquellos como si fueran la propia, dificultando así su detección y arresto. Para ello, el *hacker*, en vez de realizar sus consultas a Internet, hace que uno o varios de los infectados lo hagan por él y después le envíen la respuesta. Incluso puede decidir utilizar aquellos que estén conectados pero no estén consumiendo ancho de banda —por ejemplo, porque su dueño no está usándolo—. El problema de este uso es que si uno de los equipos comprometidos está en manos de la policía, puede rastrear de forma relativamente fácil el lugar del que han salido las conexiones y encontrar así lo que se conoce como *servidores de mando y control*, esto es, el lugar desde el que se dirige toda la *botnet*. Por eso los criminales, en vez de realizar la petición directa desde su centro, hacen dos o tres saltos previos, de forma que cada uno lleve a otro ordenador infectado de los, en ocasiones, miles a su disposición.

Otro de sus usos más sofisticados es guardar en los zombis porciones de archivos, como una suerte de disco duro virtual. Esto se hace con un sistema redundante para compensar la posible entrada y salida de equipos de la red. De esta forma, aunque alguien detecte lo que está ocurriendo y elimine la infección —con frecuencia, la única forma de hacerlo es volver a instalar un sistema operativo, esta vez legal, tras formatear el disco duro—, los datos seguirán a salvo.

Más común es utilizar los ordenadores infectados para enviar correo electrónico no deseado. Estas redes de zombis son responsables de la mayor cantidad de mensajes que nos invitan a comprar falso Viagra o que nos informan de que una señorita rusa imaginaria quiere conocernos. En 2011 las autoridades de Estados Unidos desmantelaron, con la inestimable colaboración de Microsoft, la *botnet* Rustock, que había operado desde 2006. Tenía bajo su *control un millón de ordenadores en todo el mundo, cada uno de los cuales, enviaba veinticinco mil mensajes por hora*. Entre el *spam* se incluían de vez en cuando archivos con un troyano. Si el incauto lo ejecutaba y no tenía antivirus, comenzaba a su vez a ser parte de la red. Los especialistas de Microsoft, después de varios meses de investigación, lograron ubicar los servidores de mando y control, que estaban en cinco ciudades estadounidenses. También la policía holandesa aisló los que se encontraban en su territorio y las autoridades chinas colaboraron para bloquear los dominios de Internet que Rustock utilizaba para funcionar. También la farmacéutica Pfizer, perjudicada por los falsos anuncios en su nombre, la empresa de seguridad FireEye y la Universidad de Washington trabajaron en la operación. Se calculó que hasta el cuarenta por ciento

de todo el tráfico mundial de correos no deseados procedía de esta red.

Una función de nuevo cuño que tienen las *botnet* es la minería de Bitcoins, como vimos en el capítulo anterior. Como hace falta mucha capacidad de proceso para conseguir realizar el cálculo de seguridad a tiempo, un *hacker* que haya tomado el control de doscientos o trescientos equipos tiene una buena oportunidad de hacer un dinero rápido. Otros han sido más agresivos y han diseñado *botnets* para robar los monederos virtuales de terceros.

Aunque, sin duda, el propósito estrella es realizar ataques distribuidos de denegación de servicio. Es una de las acciones más típicas y molestas que llevan a cabo los *hacktivistas* y, aunque no causan un daño en equipos, sí que pueden causar pérdidas millonarias por la bajada de actividad de las webs involucradas. Consiste en dejar sin servicio un sitio determinado de Internet. Una forma de hacerlo es tener las claves que dan acceso al servidor donde se aloja y, una vez dentro, eliminar su contenido. Ante una página con una protección media esto es muy difícil y, además, puede ser solucionado en cuestión de horas en el peor de los casos. Hay otra forma de evitar que nadie la pueda ver. Una web recibe peticiones de contenido de otros lugares del mundo a las que va respondiendo en orden de llegada. A cada una le envía una serie de datos —que suele ser su propio contenido, lo que cada uno visualizamos en el ordenador—. La cantidad de peticiones que puede responder al mismo tiempo depende de la capacidad de proceso del lugar en que esté alojada y del ancho de banda del que disponga, que suele ser muchas veces superior al de cualquier equipo doméstico. Para saturarlo, solo necesitamos enviar las suficientes peticiones a esa web para que sea incapaz de contestarlas a todas, por ejemplo si tenemos a nuestra disposición otra conexión de capacidad similar a la que queremos dejar fuera de servicio. Es algo parecido al ataque a las conexiones inalámbricas del hotel con el que hemos abierto este capítulo. Eso se conoce como *ataque de denegación de servicio básico o simple* y es fácil de contrarrestar. Una vez que el defensor sabe qué dirección IP le ataca, le basta con bloquearla, ordenar al sistema que no haga caso a ninguna petición de la misma. La situación se complica si el ataque se lleva a cabo de forma *distribuida*, desde cientos de ubicaciones diferentes al mismo tiempo, situadas en cualquier lugar del mundo. No hay una pauta que permita realizar una defensa preventiva. Lo único que precisa el atacante, por tanto, es tener a su disposición una *botnet* que no necesita ser muy grande, pero sí muy dispersa, en cuantos más países diferentes, mejor. Hay empresas que ofrecen esos servicios en foros para *hackers* dentro de TOR. Ni siquiera es necesario tener los conocimientos necesarios, tan solo pagar por ello. Aunque hay un rango de precios bastante amplio, algunas de las más fáciles de encontrar cobran el equivalente a doscientos dólares en Bitcoins para saturar durante un día un sitio web cualquiera.

El portal de Internet sobre información general Prnoticias, conocido por su mordacidad a la hora de informar sobre otros medios, recibió, entre septiembre y octubre de 2013, miles de peticiones por segundo de ordenadores ubicados por todo

el mundo. La intensidad de las solicitudes fue tan grande que se desconectaron de Internet. Esto le costó a la empresa, según sus propias estimaciones, entre ancho de banda consumido, pérdida de reputación y reclamaciones de los anunciantes, cuatrocientos veinticinco mil euros. Todos los intentos de volver a operar fueron infructuosos, así que pusieron la correspondiente denuncia ante el Grupo de Seguridad Lógica de la Unidad de Investigación Tecnológica de la Policía Nacional, que inició las investigaciones. Como todas las de ese grupo, no fueron sencillas. Se enfrentan cada día a los mayores expertos de Internet a los que a menudo les derrotan en su propio campo.

Después de veintiún días, el servicio volvió a la normalidad. El ataque había cesado y las pistas eran escasas. Un testigo declaró que un directivo de un grupo rival amenazó a su homólogo de Prnoticias con buscar «un *hacker*» para «tumbarlos» si no dejaban de publicar informaciones contrarias a sus intereses. Pero un indicio no es una prueba y, a pesar de los esfuerzos, parecía que el atacante iba a salirse con la suya.

El trabajo y los casos seguían surgiendo. Uno de ellos, liderado por el FBI, llevó a la detención de un nacional libanés en Beirut, Sami Mukahhal. Era habitual del portal de seguridad informática *hackforums.net*, donde se ofrecía como contacto de una «empresa» que realizaba por precios módicos denegaciones de servicio. Había varias transacciones económicas enviadas desde España, así que desde nuestro país se tramitó una comisión rogatoria para obtener todos los datos y estudiarlos con atención. Una vez en su poder, los especialistas de Seguridad Lógica descubrieron cinco envíos a través de Western Union, uno de trescientos ochenta y un euros, dos de doscientos noventa, otro de ciento treinta y cinco y un quinto de ochenta. En total, mil ciento setenta y seis euros. Quien lo enviaba era una mujer, desde Madrid. No había nada en ella que pudiera implicar alguna relación de cualquier tipo con el sitio atacado, lo que despistó a los investigadores. También encontraron unos correos electrónicos en los que se encargaba realizar el ataque y comunicaba los números de localización de las remesas. La empresa que gestionaba esa cuenta de *email* estaba en Canadá, por lo que tuvieron que solicitar una nueva comisión rogatoria, esta vez a ese país. La primera sorpresa fue que las direcciones IP les condujeron a Tarragona, a casa de un informático que tampoco parecía tener relación con los atacados ni con la pagadora. La pieza que faltaba en todo el puzle la encontraron al estudiar esos correos electrónicos. Hablaba sobre organizar el ataque con otro especialista en ordenadores con el que tenían una pequeña empresa en común, este residente en Madrid… y pareja sentimental de la mujer. La conexión entre los tres quedaba, pues, clara, pero aún faltaba conocer el motivo, algo que quedó dilucidado al descubrir que este último trabajaba para la subsidiaria de una empresa rival. Así, pues, se dispuso el operativo que incluyó la detención de los tres principales implicados y el registro domiciliario de la casa de los madrileños, donde se encontró material informático muy interesante para su posterior análisis. La mujer negó saber para qué o quién eran los pagos por

Western Union que le encargaba realizar su pareja. La declaración de este fue más jugosa. Explicó cómo estuvo en reuniones en que los máximos jefazos mostraban su hartazgo por las filtraciones continuas sobre ellos que aparecían en Prnoticias y que les perjudicaban, por lo que encargaron una forma de *tumbar* el portal rival. El detenido habló con su amigo, que había conocido al *libanés* en *hackforums* y sabía que este les podía hacer el encargo sin problemas gracias a su propia *botnet*. El tarraconense se encargaría del contacto con el extranjero mientras él servía de enlace con sus contratistas, de los que recibía el dinero que hacía llegar después a través de las remesas a Beirut. Un directivo fue citado y detenido por estos hechos, que siempre negó, incluso llegando a publicar un comunicado de prensa. También otros jefes de la compañía pasaron por Comisaría, aunque ningún otro fue imputado. El caso continúa en tramitación en los juzgados. Los abogados de una y otra parte siguen la pelea; el trabajo de la UIT ya concluyó al encontrar quiénes y cómo llevaron a cabo los ataques. Sorprende lo barato que resulta, por poco más de mil euros, causar un perjuicio cientos de veces superior a un rival, aunque la impunidad está lejos de existir. No obstante, hasta que no sean condenados en un tribunal, ninguno de ellos puede ser considerado culpable.

CUANDO LA SEGURIDAD CORPORATIVA ES LO QUE FALLA

La mayor cantidad de denuncias que hacen en España las empresas corresponden a robos de datos, lo que se conoce como *espionaje industrial*, y son de fácil solución. Suelen ser empleados que han terminado la relación con la compañía, despedidos, porque han terminado el contrato o porque se han establecido por su cuenta, y que conservan los permisos para acceder a los servidores. Por eso, la primera pregunta que hacen los agentes de la UIT es: «¿Quién tiene las contraseñas de acceso?». Acceder a un sistema informático no es tarea fácil para la mayoría de usuarios de Internet, hasta para los expertos. Solo hay dos formas de entrar, aprovechar una vulnerabilidad del *software* o conseguir las claves de alguna manera. La más sencilla, con diferencia, es la segunda, para la que entra en juego en muchas ocasiones la ingeniería social: hay que engañar a quien las posee para que las entregue. Eso se puede conseguir mediante la vieja técnica del *phishing* —enviando un correo al trabajador que las posee simulando que es el servidor quien las pide— o, de forma más compleja, instalando un troyano en el ordenador de un particular que capture todos los *passwords* que se tecleen, lo que se conoce como *keylogger*, grabador de claves, en inglés.

A la hora de utilizar errores de *software* tiene una importancia muy alta lo que se conoce como *inyección de SQL*. SQL, siglas en inglés de Lenguaje Estructurado de Consultas, es un sistema de programación de uso casi universal para interactuar con bases de datos. Un atacante puede utilizarlo contra su programador si la página

contiene un formulario para introducir texto. Un cuadro de búsqueda o un campo para teclear datos personales y registrarse sirven a este propósito. El truco consiste en introducir en los espacios destinados a escritura, en vez del nuestro nombre, o lo que corresponda, órdenes en SQL y que el sistema, por su mala programación, las interprete como tales en vez de como datos externos introducidos. Por ejemplo, se podría inyectar un código para que la base mostrase en pantalla los datos personales de todos los usuarios que pertenecen a la misma. Por supuesto, existen medidas sencillas que impiden que cualquier orden enviada desde el exterior pueda ejecutarse, pero requieren conocimientos por parte del responsable de la página, algo que en algunos casos no se cumple, porque uno de los negocios con más intrusismo es el de la informática.

Cuando, de una forma u otra, el atacante ha conseguido acceder, lleva a cabo el segundo de los ataques más típicos en Internet, el *defacement* o desfiguración, esto es, sustituir el contenido real del sitio atacado por uno que instalen los *hackers*, que suele ser reivindicativo. En ocasiones es el logotipo del propio grupo que haya llevado a cabo la acción y, en otros casos, una soflama de algún tipo de *hacktivismo* del que hablaremos en el capítulo diez de este libro. Ya vimos en el capítulo tres cómo los informáticos serbios realizaron este tipo de acciones contra intereses de Estados Unidos y sus aliados. Son tan sencillas como poco efectivas, ya que se puede recuperar el control y reinstalar la página original en cuestión de minutos. Horas en el peor de los casos.

Más peligrosas pueden ser las alteraciones de las bases de datos alojadas en las web a las que un atacante que haya vulnerado toda la seguridad tiene acceso. Podría, por ejemplo, bajar los precios de los productos de un comercio *online* que le interesen a un céntimo o menos y luego realizar compras que arruinen a la empresa. También podrían borrarla entera o extraer y publicar datos privados de los clientes. A finales de mayo de 2016, la web de la Mutualidad de la Policía sufrió un ataque de este tipo. Un grupo de *hackers* consiguió las contraseñas del mismo y reveló los datos personales de los cuatro mil quinientos agentes que estaban suscritos. El sitio *mupol.es* era gestionado por una empresa privada cuya seguridad, según explicaron los atacantes en su comunicado, era escasa, comenzando por la forma de acceder al servicio, con nombre de usuario mupol y contraseña Mupo2003. Eligen para sus acciones sitios fáciles, con poca seguridad y que puedan dar buenos resultados publicitarios. La seguridad corporativa de las páginas oficiales de la policía es mucho más difícil de romper. Además, hay una presencia constante de informáticos en el Centro de Proceso de Datos de El Escorial, donde se centralizan los sistemas policiales que, en un caso extremo de riesgo, podrían llegar a desconectarlos de Internet hasta que cesara el ataque, impidiendo de esta manera que obtuviesen dato alguno.

CUANDO ES LA POLICÍA LA QUE HACE DE *HACKER*

La nueva Ley de Enjuiciamiento Criminal permite lo que denomina «registros remotos de equipos informáticos» en su Capítulo IX del Título VIII. Esto, ni más ni menos, consiste en la instalación de un troyano que permita observar todo el contenido del disco duro sin necesidad de acceder de manera física al mismo —en el transcurso de una entrada y registro formal—. Es una medida menos intrusiva pero también menos efectiva y que requiere unas condiciones que en muchas ocasiones no se dan. Las medidas judiciales van acotadas en tiempo y forma. Por ejemplo, la intervención de un teléfono suele dictarse por periodos de un mes. Un registro domiciliario está limitado a un día determinado y ha de estar presente el letrado de la Administración de Justicia. Los agentes no tienen una realidad informática diferente a la de otro ciudadano y el envío de un troyano para lograr acceso puede no tener éxito —el usuario lo descarta o el antivirus lo detecta— o puede que lo active semanas o meses después. También es posible que, después de instalarlo, apague el equipo y solo lo utilice en periodos nocturnos, cuando ningún miembro de la judicatura va a estar disponible, salvo emergencias. Una forma más eficiente de conseguirlo es instalar el *bicho* de manera física, acceder a donde se encuentre ubicado el ordenador y, en ausencia de su dueño, colocar y activar la herramienta espía. Esto solo es viable cuando se encuentran en un sitio público, puesto que vulnerar la inviolabilidad del domicilio, uno de los derechos fundamentales que consagra nuestra Constitución, para instalarla, es igual o más perjudicial que llevar a cabo el registro formal.

En 2013 una investigación de la Brigada de Investigación Tecnológica detectó que desde un locutorio de Málaga alguien estaba dedicándose a enviar pornografía de menores. Al desplazarse agentes especializados en delincuencia informática de la Policía Nacional de aquella ciudad no tardaron en detectar a un viejo conocido que ya había sido detenido en otras cinco ocasiones por hechos similares. La lógica dictaba que era él quien tenía que estar haciéndolo, pero la justicia entiende de pruebas, no de suposiciones. El ordenador que utilizaba volvía a valores de fábrica cada vez que se apagaba —un procedimiento típico en los locutorios, por seguridad—, por lo que no se podrían encontrar evidencias en el mismo. Por ello, la única manera era instalar un troyano de tipo *keylogger* que cada tres segundos capturaría una imagen de lo que mostrase la pantalla. Era la primera vez que se utilizaba ese método en España para investigar abusos a menores. Todavía no se había modificado la Ley de Enjuiciamiento Criminal, por lo que no se contemplaba el caso de manera explícita. El juzgado lo asimiló a una intervención de las comunicaciones —que, de hecho, es lo que era, salvo que telemáticas en vez de telefónicas, las más interceptadas habitualmente— y autorizó treinta días de vigilancia con las restricciones de que el detenido siempre tenía que usar el mismo equipo y solo podía hacerlo él —dado que sería ilegal violar el secreto de las comunicaciones de otros no investigados—. Contando con la anuencia del dueño del establecimiento, los agentes instalaron el

programa en el equipo preferido por el pedófilo. Al hacerlo ellos, no era necesario esperar a que lo activase, sino que desde ese momento, tuvieron acceso a todo lo que hacía. De este modo encontraron pruebas no solo de su actividad como distribuidor, sino de su contacto con otros interesados en las mismas imágenes y, peor aún, del acoso al que sometían a niños que encontraban en Internet para obtener imágenes sexuales de ellos, incluso coordinándose entre sí. Las evidencias fueron tantas y tan alarmantes que una semana después de su inicio, los agentes dejaron de usar el troyano y procedieron a su detención. Ante los hechos probados y de los que quedaban imágenes grabadas, ingresó en prisión. Un año después la investigación culminó con otras tres detenciones en España, se informó a través de Interpol a varios países latinoamericanos donde había otros miembros de la trama y se identificó a un cierto número de menores engañados.

Ahora los policías, a pesar de todos los inconvenientes, disponen de herramientas que hasta hace poco solo estaban al alcance de los que se encuentran al otro lado de la ley. Gracias a ellas van a lograr descubrir delitos que hasta el momento quedaban impunes.

9

LA VOZ DE LOS NECIOS

Daniela mira la pantalla de su móvil con atención. Es la única luz de la habitación a oscuras. Es madrugada. Si sus padres supieran que no está dormida, se enfadarían. Pero no tiene sueño. A pesar de sus trece años, su familia, sus amigos y sus excelentes notas en el colegio, tiene preocupaciones que la mantienen en vela. Como muchas adolescentes, se siente insegura sobre su cuerpo, que tantos cambios está teniendo. Empezó a mirar cuál sería el peso ideal de alguien de su edad. Creía que tenía un poquito más de la cuenta, así que buceó en la Red. Los primeros resultados eran demasiado médicos, demasiado fríos. No tardó en encontrar otros que estaban escritos para ella. Aprendió qué era una princesa, quiénes Ana y Mía. Comprendió, con horror, que sus cuarenta kilos para su metro treinta y cinco eran una horrible exageración. Estaba gorda. Internet se lo decía y lo escrito siempre tiene más peso que los elogios de su tía o esas miradas de los chicos de su clase que no sabía interpretar. El mundo no la entendía, no era consciente de su problema, de su obesidad. Por fortuna, había muchas otras chicas como ella que sabían lo que tenían que hacer. Hablaban con seguridad y las creía, sobre todo porque conocían desde dentro lo mismo que ella estaba sufriendo. Aprendió los trucos básicos, como esconder comida en la servilleta, darle los mejores trozos al perro cuando nadie miraba, explicar que había merendado mucho en casa de alguna amiga para no cenar. Al principio fue difícil. Solo al principio. El estómago gruñía hasta que supo dominarlo, enseñarle que era mejor el beneficio. En pocas semanas había rebajado varios kilos. Su madre preguntaba si se encontraba bien. Daniela a veces no tenía energía —ella lo llamaba «ganas»— para salir de casa. Hasta desfalleció un día en Educación Física. Le dijo al profesor que estaba teniendo una regla muy dolorosa, como había leído en una de sus páginas favoritas. Coló. Lo cierto es que hacía meses que la menstruación, que nunca había sido muy regular, ya no bajaba. Su padre la veía como un esqueleto, casi de manera literal, pero ella, instigada por sus sabios invisibles de más allá de la pantalla, notaba exceso de grasa aquí y allá. Su tripa era un agujero entre los pulmones y el coxis. Sus nalgas tan escasas que le dolía estar sentada sobre los huesos más de diez minutos. Participó en carreras de kilos donde las chicas y algún chico publicaban lo que bajaban día a día durante una semana. Quien adelgazaba más ganaba. Ella siempre perdía porque no había ya de dónde rebajar.

Esa noche, desesperada por su fracaso lee el consejo definitivo: beber un pequeño trago de detergente para la vajilla, porque, como dice su publicidad, «disuelve la grasa». Lo pone en práctica a la hora del desayuno. No puede ir al instituto. Pierde el conocimiento y casi la vida en el suelo de la cocina, donde la

encuentra su hermano pequeño, que, con sus gritos de pánico, atrae a los adultos que la llevan sin protestas —porque para quejarse hay que estar despierta— al hospital. Los médicos se asustan de su estado, casi crítico, no solo debido al lavaplatos sino a la falta de nutrientes de su organismo. No dan demasiadas esperanzas a sus padres. Pero Daniela es fuerte. Estará ingresada casi dos años, no por los perjuicios físicos, que los superará pronto —aunque tendrá secuelas todas su vida, entre las que estarán una corta estatura y daños en el sistema digestivo—, sino por su trastorno alimentario, de origen mental. Anorexia nerviosa lo llaman los doctores. Estará con supervisión para que coma como debe todo ese tiempo. Saldrá con miedo de recaer. Habrá aceptado que la imagen que le devuelve el espejo no es la real, pero no sabrá interpretar nunca cómo debería ser. Esperará mantener la principal promesa que le hizo a su terapeuta, no volver jamás a buscar en los foros de Ana y Mía.

EL RIESGO DE LA CREDULIDAD

Internet ha permitido que todo el que lo desee pueda contar al mundo lo que piensa. Cualquiera puede abrirse un blog o un canal en un portal de vídeos y opinar de lo que sabe y de lo que no. No se pide un certificado de conocimientos. No es necesaria una experiencia demostrable en un campo determinado. Los ignorantes suelen escribir de forma sencilla y accesible, atrayente para quien tampoco tiene una suficiente formación ni espíritu crítico. De esta forma consiguen una repercusión notable, en ocasiones mayor que la de los propios expertos, hasta fuera de la red. Uno de los casos paradigmáticos ocurrió en Televisión Española en junio de 2015, cuando, ante la muerte de un niño por no vacunarse —de lo que hablaremos más adelante— dieron voz por igual a los médicos y a los *antivacunas*, que carecen de una sola evidencia en su favor y de la mínima formación necesaria para entenderlo. De esta forma se contribuye a sembrar el desconcierto en la sociedad y a esparcir contenidos nocivos.

Todos tienen el mismo derecho a opinar, lo mismo un premio Nobel hablando de su propio campo que un total ignorante. La libertad de expresión es un derecho consagrado en nuestra Constitución, con los límites que indique la ley. No obstante, ser libre de opinar no significa que las opiniones deban ser respetadas o tomadas en serio. Ese es uno de los errores más comunes. Las personas, por el hecho de serlo, merecen respeto. Sus ideas, no necesariamente. En Internet, las teorías de los sabios son disputadas por quienes no saben de qué se está hablando y han formado su cuerpo argumentativo con un par de experiencias personales —que no son significativas en el conjunto de la población— y las expresiones de otros cuyas ideas coinciden con las suyas, lo que los ingleses definen como *wishful thinking*, esto es, creer que las cosas son como a uno le gustaría que fueran, no como la tozuda realidad se empeña en definir.

Los sabios en cada campo no lo son por sí mismos, sino por el conocimiento que han acumulado y que pueden defender, refrendado por lo que se conoce como *método científico*, una serie de procedimientos estrictos para diferenciar la casualidad del hecho y que ya definió Descartes en el siglo XVII. Sus principios se estudian durante la educación básica en España, pero muchos lo olvidan con rapidez. Se fundamenta en evitar las distorsiones que la propia naturaleza humana introduce en las observaciones, lo que se conoce como *predisposiciones* o *sesgos cognitivos*. Somos seres destinados a sobrevivir en un entorno pequeño que hemos superado nuestra propia limitación. Eso requiere también modificar la manera en la que analizamos la realidad, porque nuestra percepción subjetiva está obsoleta.

Dicho de una forma sencilla, el método consiste, en primer lugar, en *observar* un determinado hecho o fenómeno, tomando las debidas anotaciones para su sistematización. A continuación, basándonos en lo observado, formular una explicación provisional llamada *hipótesis*. El siguiente paso consiste en ponerla a prueba mediante experimentos, tratando de confirmarla o desmentirla a través de todos los escenarios posibles. Este paso es muy probable que muestre alteraciones a la hipótesis planteada, que se describen en lo que se conoce como *antítesis*. La sistematización del conocimiento adquirido, la explicación rigurosa de lo que acontece y cómo acontece es lo que se llama *tesis* o *teoría*. Es decir, una *teoría* es la aplicación de unas hipótesis en un conjunto de reglas verificables por un tercero y que explican un determinado fenómeno o realidad. En las condiciones actuales, la fase de experimentación es tan minuciosa que puede durar años o hasta décadas y tiene múltiples supervisiones y controles por parte de otros equipos de investigadores. La ciencia es siempre duda, nuevos interrogantes que resolver y nuevas respuestas que dar. A medida que tenemos más conocimientos, viejas teorías van quedando atrás. Eso no es porque quienes las desarrollaran fueran laxos, sino porque no tenían los medios actuales.

Un artículo informativo correcto, en Internet como en los demás sitios, está avalado por estudios realizados por especialistas que son citados y pueden ser consultados. Con este espíritu nació la popular Wikipedia, aun con todos sus conocidos problemas que no la convierten en el más fiable de los textos. Sus normas de edición exigen que cada afirmación esté respaldada por las palabras de un especialista que se puedan comprobar, además de mantener una estricta neutralidad y aportar diversos puntos de vista cuando sean relevantes. La teoría es excelente, pero dado que cualquiera puede redactar esa enciclopedia del conocimiento compartido, es fácil que malintencionados o tan solo equivocados escriban sus opiniones como pruebas reales, sin citas o con referencias a sitios sin valor científico.

En Internet todos los participantes están al mismo nivel. En una discusión sobre medicina en un foro cualquiera tiene la misma relevancia la aportación de un médico que la de alguien cuya única relación con la materia es que estuvo tres días ingresado en un hospital. Este, además, puede tener una opinión más cómoda de aceptar por la

mayoría, en especial por su sencillez, lo que la hace más popular, e incluso puede conducir al descrédito virtual del mejor formado. Por eso es habitual que los expertos dejen de participar en foros, salvo los especializados que, o bien son privados, o bien son demasiado complejos para ser comprendidos por el lego. De esta forma, con honrosas excepciones, el verdadero conocimiento suele estar fuera de los sitios más accesibles de Internet y lejos del ciudadano medio, que prefiere creer lo simple antes de lo cierto, porque es más fácil, porque lo comprende, aunque sea erróneo y no se moleste en comprobar si lo es. Este problema se extiende a otros lugares de la sociedad. Por un lado, muchos ciudadanos siguen a su gurú favorito —político, periodista o lo que sea— como quien es forofo de un equipo de fútbol, con pasión y sin autocrítica. Da igual que la ciencia desmienta con rotundidad una afirmación, ellos se limitarán a creer y hasta defender con cerril cabezonería a su ídolo, porque no se molestarán en llevar a cabo una de las principales actividades que garantizan no ser engañado en la vida cotidiana: comparar, leer y decidir con información variada. Además está la actividad de grupos editoriales, físicos o virtuales, que saben que es más rentable tener lectores y obtener ingresos por la venta o por publicidad que contar la verdad, que suele ser compleja y difícil de aceptar. En resumen, Internet es un lugar que almacena grandes conocimientos, pero se corre el riesgo de no descubrirlos entre la ingente cantidad de contenido irrelevante o dañino.

Aquello que utiliza argumentos científicos sin que en realidad lo sean se conoce como *pseudociencia*. Se llama así porque no utiliza el método científico, sino que, en el mejor de los casos, lo retuerce para que encaje con sus objetivos. En el peor, se limita a considerar su propuesta como dogma irrenunciable y negar con diversas falacias cualquier cosa que se oponga a ella.

En el último tercio de 2014 se popularizó un vídeo en el que un señor que se hacía llamar Manuel Nava Rro (*sic*) frotaba la piel de una manzana, de la que iba saliendo una pasta blanquecina que a continuación quemaba, lo que dejaba, según él, un olor «a plástico quemado». Dudaba, por tanto, de lo idóneo de todos los alimentos que se venden en los supermercados y concluía que ni el gobierno ni sanidad vigilan en absoluto lo que pasa con la industria alimentaria. Como pasa de vez en cuando sin que se tengan claros los motivos, el vídeo se *viralizó*, es decir, comenzó a ser compartido por muchas personas por todo Internet, de manera que a principios del año siguiente había sido reenviado medio millón de veces, reproducido más de trece millones y en muchos lugares se hacían eco del mismo, indignados por tamaño peligro para el ciudadano medio.

Este ha sido uno de los últimos triunfos de la ignorancia. Los expertos como Pedro Terrón, de la página Bulos y Leyendas, y el divulgador científico Mauricio-José Schwarz, autor, entre otros, del blog *El regreso de los charlatanes*, desmintieron con datos cada una de las afirmaciones. El sector alimentario es uno de los que más control gubernamental tiene. Es fácil comprobarlo atendiendo a la cantidad de leyes aplicables, que se pueden consultar en el Boletín Oficial del Estado. Es habitual ver

noticias de que cierto producto ha sido retirado de la venta porque se había descubierto una posibilidad nimia de contaminación, desde hamburguesas con carne de caballo —que en absoluto es nociva pero se consideró un fraude al consumidor— hasta lotes enteros de conservas en las que alguna lata estaba contaminada con toxina botulínica. Hay continuas supervisiones, y no solo oficiales, sino de la propia marca, del vendedor y de organizaciones de consumidores. Bastaba también una pregunta a los expertos para aprender que las manzanas producen de manera natural una cera, que es la que le da ese aspecto brillante. En ocasiones se recubre de otra, comestible también, llamada carnaúba, que se extrae de la hoja de palma y que se usa para alargar el buen aspecto de los productos, que es inocua, cuyo uso, por supuesto, está regulado y que, al arder, produce tan peculiar olor.

El vídeo original, aunque pueden verse muchas copias, acabó por ser retirado porque «infringía la política de YouTube sobre *spam*, prácticas engañosas y estafas». Para entonces, el mal ya estaba hecho. Cuesta mucho menos esfuerzo crear un bulo que desmentirlo y, a pesar de dedicar recursos y energía, la verdad apenas llega a un veinte por ciento de quienes se lo han creído en primer lugar.

Este es uno de los muchos ejemplos de mentiras que se esparcen basadas en la ignorancia de quienes las difunden. Su daño específico es bastante bajo, poco más que algo de ruido e indignar a muchos crédulos. Cualquier persona con una experiencia media en Internet habrá encontrado muchos otros bulos, compartidos por millones. Su funcionamiento suele ser cíclico. Algunos se detectaron en los albores del Internet popular, a finales de los años noventa, y vuelven unas dos veces al año con ligeras variaciones. Uno de los más habituales es el que dice que Facebook va a ser de pago a menos que se comparta determinado texto sin ningún sentido. La primera vez que apareció no existía ni siquiera el concepto de red social. Entonces, lo que iba a cobrarse, salvo que se enviase cierto mensaje a diez personas, era Hotmail, el correo gestionado por la empresa Microsoft que permitía acceder al servicio de mensajería instantánea MSN Messenger. Otra variante pide que se comparta en cada *muro* una supuesta prohibición que impide que la empresa de Mark Zuckerberg utilice los datos privados colgados en ella. Ambas tienen la característica de que, con cinco minutos de búsqueda en Internet o incluso con un poco de ejercicio del sentido común, quedan desmentidas. Ni siquiera están redactadas de un modo correcto o hacen referencia a leyes o acontecimientos reales.

Hay bulos más peligrosos, destinados a crear alarma social. Unos son genéricos, como uno sobre llaveros rastreadores que se venden en gasolineras para robar vehículos en autopistas o el famoso «la pandilla basura», sobre una peligrosa banda juvenil que intentará asesinar a quien le haga el cruce de luces. Otros se desencadenan ante hechos concretos. De esos, el más recurrente es una amenaza de atentado que va a ocurrir en un fin de semana en un centro comercial. El lugar va variando. Lo aderezan con datos como «mi cuñado que es policía nacional me lo ha confirmado». La página en Facebook de la Unidad de Investigación Tecnológica

suele desmentir aquellos que cobran más vigor o causan más miedo en la sociedad.

Los bulos tienen una serie de características que los hacen muy reconocibles:

1. Son de origen desconocido. No se sabe quién los crea, ni cuáles son sus propósitos concretos.
2. No van firmados por ninguna persona real. Cuando aparece un nombre, es ficticio o utilizado de manera apócrifa.
3. Aluden a una necesidad básica para calar en la población, en especial el miedo (bien sea económico, bien físico o de cualquier otro tipo).
4. Suelen pedir su reenvío masivo para conseguir la mayor difusión posible.
5. Su redacción es a menudo defectuosa.
6. Los antecedentes del hecho que cuenta y sus referencias son ficticios o distorsionados.
7. No se puede encontrar ninguna referencia a lo que narra en fuentes oficiales o prensa seria.
8. Son lo suficientemente genéricos para poder encajar con mínimas variaciones en cualquier lugar del mundo y en cualquier periodo temporal.
9. Van modificando o añadiendo párrafos nuevos, con diferentes estilos. Están, por tanto, *vivos* y se comportan como las narraciones orales desde tiempos de Homero, que se *enriquecen* con las aportaciones de nuevos *autores* a lo largo del tiempo.

La policía y los expertos recomiendan seguir la regla de oro de Internet, *comprobar primero, compartir después*. Hay incluso páginas web dedicadas a investigar y desmontar estas mentiras sistemáticas, como *hoaxbusters.org* y *snopes.com* que pueden ser muy útiles para quien busca confirmar o desmentir una historia demasiado extraña para ser creída.

Los bulos, además, pueden llevar delante del juez a quien los crea, si es posible hallarlo, o a quien los comparte con conocimiento de su falsedad, dado que es un delito tipificado como desórdenes públicos si causa la suficiente alarma y obliga a la movilización de los servicios de emergencia. En noviembre de 2015 cuatro jóvenes residentes en la localidad malagueña de Estepona fueron detenidos por la Policía Nacional. Tres eran magrebíes y el cuarto ruso. Crearon y propagaron un bulo que en cuestión de minutos se difundió por WhatsApp de forma exponencial, en el que se afirmaba que era inminente un atentado yihadista en su ciudad. Para ello llegaron a realizar un montaje con la portada del diario *El País*.

MÁS ALLÁ DE LOS BULOS: LOS ENGAÑOS QUE CAUSAN MUERTES

La falta de formación y el miedo o la necesidad de creer pueden cruzar la línea entre

lo inocuo y lo mortal. Así pasa con el movimiento antivacunas, que está conduciendo a la reaparición de enfermedades que se creían olvidadas. A pesar de ser muy activo en Internet, la mayoría de la población fue consciente de su existencia en junio de 2015, cuando un niño de seis años de Olot, en Gerona, contrajo difteria, una enfermedad cuyo último caso había ocurrido en España treinta años antes, y falleció después de veinticinco días ingresado en cuidados intensivos. Los padres comparecieron poco después, para decir que se sentían «destrozados y engañados» al haber creído a una asociación que les convenció de no vacunar al pequeño. La manipulación de la que fueron víctimas le costó la vida.

La capacidad de inmunizar al cuerpo contra las amenazas más agresivas es un muy bien conocido recurso médico, que lleva centurias utilizándose. Si bien hay antecedentes de su uso contra la viruela hasta en el siglo X a. C., se sistematizó su uso a partir de finales del siglo XVIII. Fue el francés Louis Pasteur el que, en 1881, demostró de manera científica que el método era válido. De hecho, la eliminación de la única enfermedad erradicada de la faz de la Tierra, la ya citada viruela, se llevó a cabo gracias a la vacunación sistemática de toda la población, que comenzó en 1958, tras una propuesta de la Unión Soviética ante las Naciones Unidas. Otras enfermedades graves, como la difteria o el sarampión, no registran casos durante décadas. Basta dar una vuelta por países africanos para descubrir lo que pasa cuando la medicina no llega a todas partes. La poliomielitis, que deja a los niños con las piernas inútiles para toda la vida, todavía campa por sus respetos. En el Primer Mundo, donde la inmunización es casi universal, se ha convertido en desconocida. Es en este contexto, en el que los adultos ya no han conocido peligrosas epidemias que arrasaban a gran parte de la población mundial y que podían ser controladas con facilidad, en el que algunos deciden que quizá no sea bueno someter a los niños a tales cócteles biológicos y químicos. Es decir, se oponen a un remedio que está comprobado mediante el método científico, basándose solo en sus corazonadas o en ideas particulares, sin base.

El movimiento antivacunas ha estado asociado sobre todo a motivos religiosos y es casi tan antiguo como el objetivo que persigue. En la actualidad en países donde reina el integrismo islámico, los voluntarios que van repartiendo las dosis puerta a puerta han pagado con su vida las consecuencias de sus esfuerzos por salvar las de otros. En Internet, sin embargo, los principales activistas son menos agresivos —aunque sus acciones u omisiones cuesten la vida de niños— y se orientan no tanto a negar la efectividad, que ya hemos visto que está probada, sino a los riesgos de su administración, que afirman que superan a los beneficios. Estos negacionistas se basan en gran medida en un trabajo del exmédico británico Andrew Wakefield, que en 1998 publicó junto con otros doce colegas un estudio en la prestigiosa revista *Lancet* sobre la incidencia de la vacuna triple vírica, una de las obligatorias en buena parte del mundo, en doce menores que padecían autismo. Su conclusión era que la enfermedad estaba causada por la propia inoculación, que, además, favorecía otras

enfermedades intestinales. Investigadores de todo el mundo intentaron reproducir sus hallazgos sin conseguirlo en ningún caso. De hecho, encontraban justo lo opuesto, por lo que fue objeto de gran controversia —uno de los principios del método científico es que si se repiten los experimentos en las mismas condiciones, se hallarán los mismos resultados—. En 2004, un periodista de *The Times*, Brian Deer, reveló que Wakefield estaba desarrollando una vacuna alternativa y que, por tanto, tenía motivos para desprestigiar la vigente. La mayoría de los cofirmantes del estudio médico retiraron su firma y el Consejo General Médico del Reino Unido le abrió un expediente en el que le acusó de someter a los niños a técnicas invasivas no necesarias (como colonoscopias y punciones lumbares).

El estudio, muy restringido por su naturaleza técnica, saltó a la fama cuando el actor Jim Carrey y la modelo Jenny McCarthy lo citaron en 2007 al afirmar que su hijo sufría autismo por culpa de la triple vírica, para concluir que, al año siguiente, el niño se había *curado*, algo imposible con los conocimientos actuales. La repercusión atrajo a muchos padres a posicionarse en contra de las vacunas, con dramáticas consecuencias.

En 2010, un tribunal médico dio por probadas treinta y dos acusaciones contra Wakefield, cuatro de ellas por fraude, y le expulsó de la carrera, de forma que no puede ejercer. *Lancet* retiró el informe de sus fondos y dedicó un editorial a explicar sus razones. Pero el daño ya estaba hecho y Wakefield ha continuado con su labor de proselitismo, a pesar de que no hay ni una entidad con credibilidad en todo el mundo que apoye sus tesis.

Rechazar las vacunas es un riesgo tan grave y tan peligroso para la población que la propia Organización Mundial de la Salud tiene una página destinada a desmentir los bulos y leyendas urbanas que esparcen desde las asociaciones, como hemos visto, sin ningún argumento sólido. A pesar de los contundentes y probados argumentos y la desautorización completa del estudio que relacionaba las vacunas con el autismo, los *creyentes* siguen refiriéndose al mismo como si tuviera algún valor. Sus argumentos, ante la falta de otros con más peso, acaban cayendo en el rango de los *conspiranoicos* que veremos más adelante.

La presencia de los antivacunas en Internet no es muy patente para el público en general. Los seres humanos somos gregarios y tendemos a asociarnos con aquellos que tienen ideas similares a las nuestras. Basta pasearse por los foros y las páginas de sus asociaciones para encontrar un mundo alternativo en el que las tesis más peregrinas tienen cabida, siempre y cuando coincidan con su postura contraria a las vacunas. Como la ciencia tiene su camino inexorable, en ocasiones los estudios demuestran que algo no es tan efectivo como se pensaba o que debe ser retirado, como ocurrió en 2010 con las vacunas Rotateq y Rotarix, que fueron sacadas del mercado por una supuesta contaminación de virus porcino en ciertas muestras. Eso les da munición para la cruzada genérica. En su propio gueto virtual se retroalimentan y llegan a pensar que son una mayoría los que comparten su postura y los demás son,

tan solo, desinformados. De hecho, tras la muerte del niño de Olot se entablaron auténticas batallas dialécticas entre partidarios y detractores. En general, aquellos que se apartan de los estudios científicos se comportan de manera parecida a fanáticos religiosos, donde sus afirmaciones son sagradas y quien las pone en duda debe ser blanco de sus ataques. Las conversaciones en Internet carecen de dos elementos contemporizadores clave, el contacto personal y el lenguaje corporal, lo que conduce a que las discusiones escalen con rapidez a peleas e insultos y la búsqueda, en una cita libre de Miguel de Unamuno, de vencer más que convencer.

Hay otras personas que se mueven en Internet de una manera mucho más oculta, mucho más sosegada, que no salen de sus guetos para imponer sus ideas, porque son conscientes de que van a ser repudiados, de que casi nadie les apoya. Son aquellos seducidos por los contenidos nocivos que, sin ser ilegales, amenazan la vida. El mundo de *Ana* y *Mía* es tan rico como aislado y aterrador y no existiría de no haber un medio de ponerse en contacto entre sí como es Internet. Bajo esos dos nombres no se esconde ninguna persona, sino que es parte de la jerga de los chicos con trastornos alimentarios. *Ana* es la anorexia y *Mía*, la bulimia. Ellos, entre sí, se definen como *princesas* y *príncipes*. De una manera muy simplificada, la primera consiste en no comer en absoluto al recibir una imagen distorsionada del propio cuerpo, que siempre ven obeso, aunque estén en los huesos. La segunda lleva al afectado a darse atracones en muy cortos periodos de tiempo, engullendo más de lo que su cuerpo puede admitir, para a continuación entrar en fase de arrepentimiento y vomitar todo o usar laxantes para expulsarlo pronto. Son enfermedades muy graves, que pueden llevar a la muerte y que son peores en un grupo en el que se apoyen mutuamente. Fuera de sus círculos se sienten repudiados y hasta perseguidos. Ni sus familiares ni sus amigos *reales* les comprenden porque les hacen ver que su aspecto no es sano. En sus sociedades virtuales se dan apoyo y comprensión. Hablan de su enfermedad como un *estilo de vida*, no como de algo que necesite atención médica. Quienes participan en ellos son a menudo adolescentes sin conocimientos cualificados de medicina y, además, proclives a creer lo que les interesa y despreciar lo que les contradice.

Comparten algunas técnicas aceptadas como efectivas. Entre ellas, consumir tabaco o cocaína para controlar el apetito, no comer nada sólido después de las siete de la tarde o distraer el apetito limpiando sitios desagradables, como el inodoro, en especial si está muy sucio o recién utilizado. Ofrecen consejos para pasar desapercibidos a la hora de no ingerir casi nada en las comidas. Es muy popular esconder los alimentos en la servilleta para arrojarla luego a la basura con discreción y, por supuesto, que el perro se aproveche de los restos debajo de la mesa. Otras ideas más descabelladas no consiguen calar entre ellos, como la de beber un tapón de lavavajillas porque «disuelve la grasa». Aun así, siempre hay alguien que la lleva a cabo y acaba en el hospital o en el cementerio.

Sirva como ejemplo, un día de dieta sacada del blog *Una princesa suicida* (las cursivas las ha marcado el autor de este libro):

Día 2. Desayuno. Media taza de leche (intenta suprimirlo, pero no lo quites sí o sí, ya que necesitamos calcio, porque si no, este se consigue de los huesos, *queremos que se nos vean los huesos, ¡pero no rotos!* Además, ¿una desdentada? ¡Ay, no!). Un vaso con agua. *En el cole/instituto* (a eso del mediodía). ¡Agua a más no poder! Si me da hambre y siento que me desmayo, compro esos caramelitos «ticktack», menos de una caloría por 25 unidades. En la casa; almuerzo. Hoy lo suprimes. 1 vaso con agua. 11. Un té y medio paquete de galletas de soda (4 o 5 galletas). Cena. Intenta suprimirla, para esto, el 11 lo vamos a tomar a eso de las ocho de la noche.

Los *príncipes* y las *princesas* organizan sus competiciones semanales llamadas *carreras*, donde los que se apuntan van indicando cuántos kilos han perdido cada día. El ganador, por supuesto, es quien más adelgaza. Algunos protestan porque no logran seguir el ritmo de los demás, porque llevan ya meses o años y su cuerpo ya no tiene nada de lo que desprenderse, sin que hacerlo le lleve a la tumba. Definen como *dieta suave* consumir quinientas calorías al día. Insisten cada pocos mensajes en que deben mantener su enfermedad en secreto y jamás discutir con quien no crea en ello. Si otros lo saben, les «apartarán del camino de la perfección». Incluso aceptan como propias algunas de las imágenes tradicionales para advertir de su peligro, como fotomontajes en los que una chica delgada observa en el espejo su reflejo como el de una obesa.

Sus foros y blogs no están en la *deep web*. Basta una corta búsqueda con cualquier motor para encontrar cientos de resultados. Lo que está escrito da tanto miedo que existe la tentación de creer que es una especie de broma macabra, hasta que se leen los comentarios. Las aportaciones de otros, a menudo angustiadas llamadas de auxilio para perder peso, se cuentan por cientos; es decir *arrastran* a multitudes que les creen y están dispuestas a sacrificar su salud de una manera que quizá no harían si no leyeran cómo hacerlo. Son fáciles de hallar porque *no están prohibidas*, ni en España ni en la mayor parte del mundo. Como todo aquello que no está expresamente prohibido está permitido, los servidores de Internet que las alojan no están obligados a retirarlas, a pesar del esfuerzo de asociaciones de defensa de la infancia, de lucha contra los trastornos alimentarios y de la propia policía. La Unidad de Investigación Tecnológica ha conseguido que se retiren cientos de ellas, pero es algo que depende en exclusiva de la voluntad de quien las aloja, que se puede amparar en la legislación para no hacerlo. Incluso aquellos que tienen voluntad de no alojarlas pueden encontrarse con que alguien les ha abierto una, que puede pasar desapercibida durante años antes de que la detecten —por una denuncia o por un incremento inusual de tráfico de datos—. Es una de las amenazas más serias para los adolescentes que hay en todo Internet y continúa día tras día, arriesgando la vida de muchos de ellos, en especial, chicas, que son entre las tres cuartas partes y el noventa por ciento de los afectados.

Hay una amenaza más grave y directa, buscar la muerte. Muchas páginas la justifican y hasta la glorifican. Algunas, tan fáciles de encontrar como las anteriores, están tan bien argumentadas que son capaces de afectar al ánimo incluso de una persona optimista o con convicciones firmes. Tienen su reflejo en la red TOR, con sitios como Sanctioned Suicide, que se traduce como suicidio aprobado. En ese foro colaborativo, aquellos que no desean vivir pueden expresarse y encontrar apoyo, pero también —y aquí se entra en lo delictivo—, ayuda para encontrar métodos de dejar el mundo. En España, inducir a que otro se mate se castiga con penas de entre cuatro y ocho años de cárcel y de dos a cinco al que *solo* colabore con actos necesarios para que se lleve a cabo.

El 18 de mayo de 2012 apareció en un hotel de Avilés (Asturias) el cuerpo sin vida de una mujer de unos cincuenta años con tendencias depresivas, aunque en absoluto enferma terminal. Los agentes del Cuerpo Nacional de Policía en aquella ciudad detectaron una serie de anomalías que hacían pensar que podía haber alguien detrás de esta muerte. La mujer había viajado de Valladolid al lugar de su fallecimiento. Junto al cadáver había restos de un zumo de melocotón y de un potente anestésico animal. El día anterior había sacado seis mil euros en una caja de ahorros de la capital pucelana. Las personas que van a morir le suelen tener poco aprecio al dinero, algo de lo que se pueden aprovechar segundos o terceros interesados. El día anterior había hecho dos llamadas telefónicas a números que le resultaban extraños. Los investigadores rastrearon ambas. Una llevaba a una veterinaria amiga de la occisa, que contó a los agentes que esta le había dicho que tenía la sustancia mortal y quería saber si la cantidad sería suficiente. A pesar de sus intentos de disuadirla, nada consiguió.

El otro llevaba a un hombre que no se quiso identificar. Se limitó a decir que había estado en contacto con la suicida y que pertenecía a una organización «por el derecho a una muerte digna». Ante la sospecha de que pudiera planear otras muertes, se solicitó de inmediato al juzgado la intervención de la línea, que resultó pertenecer a un anciano de setenta y un años —aunque alto y de buena planta, aparentaba menos, a lo que ayudaba la vida activa que llevaba— de Barcelona. Así comprobaron que sus temores eran fundados. Estaba a punto de *ayudar a morir* a otra mujer en su ciudad, junto a la hija de esta. Se preparó un operativo en un tiempo récord para detener a ambos y proteger a la víctima. Tras lograrlo, registraron el domicilio del varón, en el que apareció gran cantidad de documentación sobre esas asociaciones —en una de las cuales, en efecto, era voluntario— y una caja de la misma sustancia que había acabado con la primera fallecida, que sospechaban que no había sido la única. El anciano, que se suicidó ese mismo año, no tuvo ningún reparo en reconocer los hechos investigados, a los que sumó dos *ayudas* a sendas personas más que también habían fenecido y a otro par a las que había entregado la medicación, aunque aún seguían en este mundo. Solo negó haber recibido el pago de seis mil euros por sus servicios, ya que decía hacerlo por altruismo. El hecho objetivo es que se encontraron

en su poder, según su declaración porque la fenecida se lo había dejado oculto en el coche a pesar de sus objeciones.

Como había mucho material informático, al que había que sumar el de la mujer encontrada en Avilés, los agentes pidieron colaboración a la BIT, que comenzó el análisis de los correos electrónicos. A través de ellos supieron que quien remitía los productos era un médico de Madrid, llamado Fernando Marín, *alma mater* de dos organizaciones cuyo objetivo era ayudar a acabar con la vida de quien lo desease, con términos como *sedación profunda* o *cuidados paliativos*. También se intervinieron sus comunicaciones y, ya el primer día, recibió una llamada telefónica en que una mujer avisaba de que «su chico» —luego se supo que estaba aquejado de esclerosis en fase muy avanzada— ya había dejado de respirar. A pesar de ser en un pueblo de la provincia, pero lejos de Madrid, el galeno se desplazó con urgencia para certificar por sí mismo que había sido una muerte natural.

Eran indicios más que racionales sobre su actividad, que se confirmaron dos días después cuando recibió la llamada de un colega, Fernando Acquaroni, que buscaba cumplir la voluntad de su hermano, enfermo terminal de sida. No tenía la capacidad de encontrar los fármacos necesarios y había recibido la negativa de los centros de cuidados paliativos legales de su provincia, Cádiz, que le habían advertido de forma explícita que lo que pretendía era un delito. Marín se ofreció a enviarle un potente cóctel de sedativos y las instrucciones para administrarlos de forma que resultasen mortales en menos de veinticuatro horas. Le explicó que, al certificar su muerte, apuntase que las cantidades para la *sedación profunda* habían sido un cuarto de las reales.

El investigado se puso en contacto con su secretaria y le pidió que enviase los productos a la dirección del colega en Cádiz. Los policías de la BIT iniciaron entonces una carrera contrarreloj para localizarlos antes de que dejasen la capital. Por fin, los interceptaron en una empresa de paquetería urgente y evitaron que salieran a su destino.

Si las drogas no llegaban, las partes sospecharían, por lo que hubo que concluir la operación. Se preparó la detención del doctor y su administrativa, y el registro de las asociaciones. Se inició esa segunda parte el 6 de julio de 2012 y hallaron una ingente cantidad de fármacos mortales. La secretaria pasó a disposición judicial.

Marín, que todavía tenía el teléfono pinchado, recibió dos llamadas consecutivas. Una era de Acquaroni, quien había sido interrogado por agentes de la Policía Nacional en su domicilio. La segunda, de un testigo que estaba dentro del local cuando entró la comisión judicial y le avisaba de que él era el siguiente. Este no perdió el tiempo y avisó a su mujer para que se deshiciera de todo lo comprometedor que pudiera haber en su domicilio. Unos minutos más tarde, la susodicha salió con una bolsa de Carrefour camino de un contenedor de basura. Lo que ella no sabía era que dos miembros de la BIT llevaban horas apostados delante de la puerta en previsión de tal eventualidad. No tuvo más remedio que entregar los productos y

retirarse. Poco más tarde, encontraron al esposo dentro de su vehículo, procedieron a leerle los derechos y lo trasladaron a la sede de la Brigada. Ingresó en prisión preventiva.

Solo faltaba saber cómo obtenía las medicinas, alguna de las cuales era ilegal en España y el resto estaba dentro de las sustancias controladas de la Lista I de Estupefacientes de la Convención de 1951 y de la Lista IV del Convenio sobre Psicotrópicos de 1971, lo que requiere un registro exhaustivo de lo que se hace con cada dosis. La respuesta estaba en los ordenadores de los detenidos en Madrid. La mujer se hacía pasar por veterinaria para comprarlos a través de Internet en México, fuera del control sanitario. Incluso tenían un proveedor habitual. El hombre, por su parte, utilizaba su carnet profesional para conseguirlos en farmacias españolas de forma irregular, ya que solo podían ser dispensados a hospitales.

El juicio se celebró en el Juzgado de lo Penal número 1 de Avilés, en mayo de 2016. Los tres acusados que seguían vivos se declararon culpables de todos los cargos y llegaron a un acuerdo con el fiscal por el que el médico y su secretaria fueron condenados a dos años y a la inhabilitación para ejercer su profesión durante seis meses y el hermano del enfermo de sida de Cádiz, a medio año de cárcel, puesto que no logró ejecutar su propósito y solo le consta como tentativa.

El derecho a disponer de la propia muerte y ayudar a otros que desean alcanzarla se debate en la sociedad actual. Se tiene especial consideración con aquellos enfermos terminales que, además, padecen un gran sufrimiento. Sobre el resto, la opinión es menos contundente. En cualquier caso, la vida es un valor supremo en nuestro ordenamiento jurídico y parece lógico que se deba intentar convencer a un suicida de que tal vez no deba dar el paso, en vez de ayudarle sin preguntar. En personas frágiles o con enfermedades mentales como la depresión, los foros dedicados a la muerte son a menudo el impulso que necesitan y que quizá no darían sin él, tras lo cual acuden a estas asociaciones sobre *muerte digna*, que también mantienen una activa presencia en Internet —algunas con webs tan obvias como *www.eutanasia.ws*—. En este caso, además, la compra de las sustancias mortales se llevaba a cabo gracias a la propia red. Aunque quien quiera morir va a encontrar una manera de hacerlo de todas formas, el mundo interconectado les da unas facilidades que antes no tenían.

CONSPIRANOICOS: EL DELGADO LÍMITE ENTRE LA CORDURA Y LA LOCURA

Dice la Real Academia de la Lengua que *conspirar* es unirse contra un particular o un superior para hacerle daño. En el derecho penal español, se define como que dos o más personas concierten la ejecución de un delito y resuelvan llevarlo a cabo. No es una palabra que tenga tintes positivos. A lo largo de los siglos ha habido muchas. Una

de las más famosas quizá sea la que documentó el historiador romano Salustio en su obra llamada, precisamente, *La conspiración de Catilina* (*De Catilinae coniuratione*), del siglo I a. C. Su protagonista, Lucio Sergio Catilina, del ala popular —defensora de los humildes, a la que también pertenecía Julio César—, había intentado repetidas veces ser elegido cónsul —máxima autoridad de la República, cuyo mandato duraba un año— y había fracasado. Cuando se quedó sin opciones, derivó hacia el populismo radical y buscó un medio de ser nombrado dictador. Para ello, a espaldas del Senado, consiguió el apoyo de un buen número de miembros de la baja nobleza y hasta comenzó a reclutar un ejército en secreto. Cicerón, el famoso orador, era el cónsul aquel año 63 a. C., y también era objetivo de los conspiradores. El 7 de noviembre mandaron asesinarlo. Por suerte para él, un senador se enteró de los planes y el político escapó antes de que los sicarios lo encontraran. Al día siguiente, en el Senado, pronunció una de sus más famosas frases, *Quousque tandem abutere, Catilina, patientia nostra?* («¿Hasta cuándo, Catilina, abusarás de nuestra paciencia?»). El interpelado amenazó a todos los senadores con causar horribles desgracias y abandonó la ciudad, en teoría hacia un destierro voluntario, pero en realidad iba a reunirse con sus tropas.

En Roma, Cicerón no podía actuar contra él porque carecía de pruebas y el huido tenía un fuerte apoyo popular y senatorial. No permitirían que se le castigara sin evidencias firmes. Así, la conspiración seguía creciendo. Una delegación de galos de la tribu de los alóbroges había acudido a pedir ayuda a la ciudad por los abusos del gobernador romano de su provincia. Eran conocidos por su potente caballería, así que los conspiradores intentaron atraerlos a su causa para que cruzaran los Alpes en el momento en que los legionarios de Catilina se pusieran en movimiento. Incluso fueron demasiado detallistas en sus explicaciones, de lo que tomaron ventaja los galos, que corrieron a contárselo a Cicerón. Consiguieron incluso que cinco senadores les pidieran ayuda por escrito. Con esas cartas, el cónsul pudo exponer por fin la conspiración y detener a aquellos cabecillas, que serían ejecutados sin juicio poco después, a pesar de un inspirado discurso del senador Julio César —simpatizante de Catilina, aunque no formó parte de la trama— en que solicitaba su perdón.

El líder, descubierto, se lanzó en un movimiento desesperado con sus tropas hacia la huida a las Galias, pero fue interceptado. Cuando la batalla quedó decidida en su contra, antes que volver encadenado a Roma, prefirió lanzarse contra el grueso de los enemigos, y falleció con varias heridas frontales, como todos sus hombres.

Podemos avanzar a lo largo de la historia y descubriremos muchas más conspiraciones, y todas tienen algo en común: han sido descubiertas. Una de las más recientes fue la que la administración Bush llevó a cabo para convencer al mundo de que en Iraq existían armas de destrucción masiva. Y es que, siguiendo la cita apócrifa de Abraham Lincoln, no se puede engañar a todo el mundo todo el tiempo.

Damos un paso más cuando hablamos de conspiraciones inexistentes, a las que un

grupo o gobierno se empeñan en dar apariencia de real. Afirman que son terribles pero tan ocultas que no se pueden demostrar, salvo prestando atención a determinados detalles. Esta falsa conjura ha sido recurrente en el tiempo y la civilización occidental está plagada de ellas, porque permiten dar respuestas sencillas a problemas muy complejos. Siempre hay un *malo* claro e identificable —aunque permanezca oculto o no se conozca su nombre— al que achacar las culpas de todo lo que sucede.

Una de las más conocidas en Europa, salvo en nuestro país, es la del *dolchstoßlegende* o mito de la puñalada por la espalda, en alemán. A partir de 1919, las élites derechistas germanas, incluyendo a muchos generales, creyeron que su derrota en la Primera Guerra Mundial (1914-1918) no se debió a ningún fallo militar, sino a que la población civil *apuñaló* al ejército en su momento de más necesidad, no solo por no ser capaces de darles la respuesta industrial que necesitaban, sino al sabotear de forma coordinada todos los esfuerzos militares con el objeto de derrocar al káiser Guillermo e imponer una república burguesa y derrotada. Los nazis, que llegaron al poder en 1933, reforzaron la mentira y la integraron en su *historia* del siglo XX, relato que sustentaba su poder. Hitler había puesto nombre a esos *traidores*. Por supuesto, judíos e izquierdistas. Durante la Segunda Guerra Mundial (1939-1945), el *dolchstoßlegende* abarcó a cada uno de los que estuvieran en su contra. A efectos prácticos, todos los opositores formaban parte de una enorme conspiración contra Alemania y debían ser eliminados. Grupos tan opuestos como comunistas, pacifistas e intelectuales de diverso pelaje, muchos de ellos sin intereses políticos y a menudo simples individuos, no podían preparar ninguna trama, porque requeriría unas capacidades de comunicación y acción absurdas por su complejidad y alcance. Eso era lo de menos, por supuesto. Lo importante era poder eliminar a todo el que no comulgase con sus ideas.

En España teníamos nuestra propia mentira, que llegaría hasta los años setenta en boca del dictador Francisco Franco, el *contubernio judeo-masónico-comunista-internacional*, a la que achacar todos los males que ocurrían. Sus protagonistas servían de enemigo exterior con el que mantener cohesionada la nación. No había lógica alguna para la asociación de tan diferentes grupos sociales y, para comprenderlo, hay que estudiar la idiosincrasia del país y de Franco. El profesor de la Universidad de Zaragoza José Antonio Ferrer Benimeli publicó en 1977 un artículo en la revista *Historia 16* que afirmaba que este había intentado entrar dos veces en la masonería en los años veinte y treinta y fue rechazado. Dado el carácter secreto de las logias de entonces y su destrucción sistemática durante la dictadura, no hay pruebas fehacientes de ello y otras fuentes lo ponen en duda o lo niegan con rotundidad. De lo que no cabe duda es de que tanto su padre, Nicolás, como su hermano Ramón sí pertenecían a ella. Las relaciones con ambos —malas, en los dos casos— o la imitación de los otros fascistas de la época pudieron influir en ese odio. El comunismo internacional, *los rojos*, fue el enemigo secular, lo opuesto al

nacionalcatolicismo que abrazaba sin pudor. La doctrina de Marx hablaba de clases sociales en vez de países y del hermanamiento de los obreros más allá de las fronteras. Además, era de un ateísmo rampante. Su fallido golpe de Estado de 1936, que desembocaría en una guerra civil de tres años que dejó devastado el país, fue contra ese modelo social, santificado en la terrible Unión Soviética. El gobierno legítimo de la República era mucho más complejo que un grupo de bolcheviques dispuestos a entregar el país a Stalin, pero eso era lo de menos. Lo importante fue perpetuarse en el poder y tener a alguien a quien echar la culpa.

Aquí entran los judíos. Al contrario de la imagen que se tiene de él, Franco no los tenía por enemigos. Al menos no al principio. En 1926 escribió un artículo para la *Revista de las Tropas Coloniales* llamado «Xauen, la triste» en que defendía a los sefardíes. Además, no había hebreos en España desde su expulsión por los Reyes Católicos. Sin embargo, en el imaginario popular, alimentado por el obligatorio dogma de la Iglesia —hasta 1959, en la liturgia de Viernes Santo se hablaba de la «perfidia judaica»—, ese pueblo era responsable de todos los males, empezando por el asesinato de Jesucristo —que él mismo y todos sus primeros seguidores fueran de esa misma religión era omitido por conveniencia—. Durante la Edad Media se les acusaba de todo tipo de atrocidades, desde las malas cosechas a la muerte del ganado o el asesinato de niños, como el inventado Dominguito de Val en Zaragoza. Así, pues, el *pueblo*, poco formado, en especial en áreas rurales, estaría más dispuesto a creer al dictador si el enemigo era reconocible en su folclore, como así fue hasta su muerte. En las teorías fascistas, además, como en el propio libro *Mi Lucha* de Adolf Hitler, se indica que los judíos son los responsables del socialismo internacionalista. En una sinécdoque criminal, como algunos judíos —entre otras personas— estaban en los puestos altos de la Internacional —Marx y Trotsky tenían esa ascendencia—, todos los judíos y nadie más que ellos eran los responsables de eso, tan opuesto al nacionalismo.

Los judíos han sido una víctima recurrente de las teorías conspirativas. Una de las más sangrantes y que sirve de inspiración tanto a Franco como a Hitler fue el llamado *Protocolo de los Sabios de Sión*, un libro publicado por primera vez por capítulos en un periódico de San Petersburgo en 1902, por el conocido editor racista y antisemita Pavel Krushevan. Simula ser las actas de unas supuestas reuniones de las élites de los hebreos en las que proponen hacerse con el control de la masonería y el comunismo para, de esta forma, lograr el gobierno de todo el planeta e imponerse con férrea mano de hierro. La policía política de los zares lo utilizó con fuerza para la represión de la población de esa religión y, a partir de 1917, de una forma muy parecida al *dolchstoßlegende* alemán, fue utilizado para culparles de los desastres de la Primera Guerra Mundial en Rusia. Se imprimieron hasta cuarenta y tres ediciones distintas, ya que también entró en el argumentario nazi y ultraderechista europeo.

Su autenticidad, ya dudosa por el carácter autoinculpatorio del mismo, se cayó a pedazos en 1921, cuando el prestigioso periódico *The Times* de Londres, entre el 16 y

el 18 de agosto, sacó una comparación entre el texto ruso y el libro francés *Diálogo en los infiernos entre Maquiavelo y Montesquieu*, escrito por Maurice Joly y publicado en Bruselas en 1865, utilizado para criticar al emperador de Francia Napoleón III. En él, los conspiradores eran otros, pero los originales fueron sustituidos por los judíos para el libelo en cuestión. El plagio llegaba a tal extremo que varios párrafos eran traducciones literales del original y hasta el esquema de los diecinueve primeros *protocolos* copiaba el de los diecisiete capítulos del *Diálogo*. En círculos conspiranoicos de Internet aún se cree en la existencia de la terrible organización secreta de judíos, dado que, por la teoría de la probabilidad, algunos hechos se han cumplido o se puede estimar que así lo han hecho.

Desde los años sesenta a la actualidad las teorías conspirativas se han secularizado. En términos generales, han dejado de servir a los propósitos de un gobierno para defender intereses particulares, a menudo ficticios. Desde el asesinato de Kennedy a las muertes de Elvis o de Marilyn. En ocasiones hasta han pasado de lo minoritario a la cultura popular en forma de leyendas urbanas. Con la llegada de Internet, todos estos grupúsculos aislados que se reunían en sociedades secretas para evitar ser descubiertos por el *gobierno*, el *poder* o cualquier otro elemento abstracto, se han podido juntar y coordinar y dar pábulo a mayores y más complejas teorías. Todas tienen una serie de patrones comunes que son fáciles de detectar:

1. *La falta de formación de quien la emite o quien la cree*. Con un poco de cultura, científica, histórica o social, la base de la conspiración cae por sí sola.
2. *El análisis simplista de la realidad*. La realidad, al contrario de lo que defienden, se explica por procesos muy complejos y usualmente ligados entre sí. Si hubiera una solución fácil para un problema cualquiera, hace tiempo que se habría aplicado. Si el problema persiste, es más fácil que no haya una manera de resolverlo que pensar en una conspiración enorme para que exista.
3. *La extrema complejidad del complot*. Para que se cumpla lo propuesto es necesaria la combinación de una gran cantidad de factores que, además, involucran a cantidades inmensas de gentes con ideas y objetivos vitales muy diferentes, que, de alguna manera, se ponen de acuerdo solo para ese propósito en particular. Cuanta más gente participe, más fácil es que uno solo lo cuente y todo se descubra, como pasó en el Watergate, por ejemplo. Del mismo modo, para que la conspiración sea posible hace falta invertir unos recursos muy grandes, a menudo más que el posible beneficio obtenido.
4. *Los responsables son entes abstractos*. Detrás de la presunta organización están grupos despersonalizados, como «el gobierno», «el Club Bilderberg», «los judíos», «los masones», el genérico «ellos» o incluso especies alienígenas o *de diferente evolución*, como «los reptilianos».
5. *Los objetivos son grandiosos e imposibles*. A menudo tienen que ver con planes

como la dominación mundial, y otras veces la motivación no queda clara, más allá de modificar nuestro modo de vida de forma irrevocable.

6. *La teoría es autoexplicativa*. Todo cabe dentro de ella y se explica por sus propios medios. Cualquier hecho es susceptible de acabar encajando en la misma. No se acepta ninguna solución que no forme parte de ella, por más evidencia científica que tenga, y aquellos que se oponen son sospechosos inmediatos de ser siervos de quienes la han organizado.
7. *Se crea alrededor de hechos de gran relevancia popular*. Siempre gira alrededor de sucesos televisivos u observables con facilidad para explicarlos a través de grandes secretos que no deben ser revelados. Sería de suponer que los movimientos secretos no intentasen llamar la atención de esa manera, para no atraer a quienes desean desenmascararlos.
8. *Utiliza hechos simples ciertos para explicar otros complejos e inciertos*. Los conspiranoicos relacionan entre sí sucesos sencillos y ciertos que no tienen nada que ver y los usan como pruebas fehacientes de otros grandes y ocultos que ni siquiera existen o pueden existir. Omiten la comprensión global de los acontecimientos, que desarmaría la teoría.
9. *Hacen preguntas para las que ya tienen las respuestas*. Los defensores de las teorías conspirativas afirman que ellos «solo hacen preguntas», pero solo aceptan las respuestas que han diseñado para ellas y rechazan cualquier otra.

Teorías conspirativas en Internet hay tantas que sería imposible enumerarlas una a una. Van desde lo más trivial a lo importante y en algunos casos han sido sustentadas por algunos medios de comunicación para conseguir más audiencia. El candidato presidencial a la Casa Blanca del año 2016, el magnate Donald Trump, ha hecho a menudo referencia a algunas de ellas, como la de las vacunas que causan autismo, de la que hemos hablado al comienzo de este capítulo y de la que está demostrado su error.

La conspiranoia paradigmática es aquella que afirma que el hombre no llegó a la Luna en 1969 ni en ningún momento posterior, que todo fue un montaje para intentar superar a la Unión Soviética, que hasta ese momento llevaba la delantera en la carrera espacial. Uno de los más desacreditados defensores, el cineasta y periodista Bart Sibrel, atrajo al astronauta Buzz Aldrin, segundo hombre en nuestro satélite, a una entrevista falsa en la que le insultó al negarse a entrar en su juego. Aldrin le lanzó un puñetazo que le alcanzó en la mandíbula, que sirvió de base para un caso penal que fue desestimado al considerar que Sibrel le había provocado a propósito.

Los defensores de la teoría afirman que las imágenes que dieron la vuelta al mundo habían sido grabadas en un estudio, dirigidas por Stanley Kubrick, y que había numerosos errores, como que no se vieran las estrellas al fondo o que la bandera pareciese ondear en un lugar sin viento ni siquiera atmósfera. Cada una de

las dudas ha sido desmontada por observadores imparciales con conocimientos de física o fotografía, lo cual no disuade al que elige creer como si fuera una fe. De hecho, quizá la prueba más obvia es que el Kremlin no desmintió el logro, a pesar de que monitorizó todo el proceso y era el más interesado en dejar en evidencia a su secular enemigo. Desde entonces varias sondas espaciales —incluida la japonesa Selene— han realizado fotografías de los lugares de aterrizaje en los que se distinguen no solo las banderas y los módulos lunares, sino incluso las pisadas, inalteradas en un lugar sin vida y sin atmósfera.

La variante de la teoría afirma que en realidad estuvieron allí, donde encontraron una civilización extraterrestre, lo que les obligó a fingir en la Tierra para no dar a conocer a la población estos hechos. Visto lo que se logra con cualquier telescopio, no merece más comentarios.

Una de las teorías más seguidas y, a la vez, más absurdas, es la conocida como *chemtrails* o estelas químicas. Afirma que esa nube blanca y larga que dejan los aviones en el cielo desde los años noventa en realidad son compuestos químicos destinados a perjudicar a la población de alguna manera que no queda clara. Algunos dicen que tiene propósitos de control de la natalidad y otros que sirve para modificar el clima, entre varias posibilidades. No está claro quién lo lleva a cabo, pero el fenómeno es intenso y global. En realidad, los aviones dejan esas características estelas de condensación detrás de sí cuando vuelan a partir de los ocho mil metros. Los motores de los aviones queman hidrocarburos que dejan dos residuos principales, dióxido de carbono y vapor de agua. Cuando ese segundo elemento es proyectado en ambientes muy fríos, por debajo de los treinta y seis grados y medio bajo cero, se cristaliza, formando una «nube instantánea». Hay grabaciones de la Segunda Guerra Mundial en las que los bombarderos que iban camino de Alemania ya dejaban esas estelas; y hay más: habían sido ya descritas tan pronto como en 1918. Defienden los conspiranoicos que lo que diferencia a las inocuas de las dañinas es que las segundas duran más. El Atlas de Nubes de la Organización Meteorológica Mundial del año 1975 ya indicaba que pueden permanecer largo tiempo en determinadas condiciones atmosféricas, hasta ser indistinguibles de los cirros. Tampoco los análisis en el suelo han detectado variaciones significativas en su composición, aunque algunos *creyentes* no sepan interpretar los datos, dada su escasa formación científica. Y, por supuesto, una vez más, los conspiranoicos dejan a un lado la necesidad de que decenas de miles de personas se pongan de acuerdo para hacer algo y ni una sola en todo el planeta se vaya de la lengua.

En España la teoría de la conspiración por excelencia tiene que ver con un hecho muy triste y lamentable, los atentados del 11 de marzo de 2004 en Madrid, cuando unos islamistas colocaron mochilas rellenas de explosivos en varios trenes y causaron casi doscientos muertos y dos mil heridos. Había elecciones generales cuatro días después y el gobierno, presidido por Aznar, en un principio defendió la tesis de que había sido la banda terrorista ETA, aunque poco después la vía yihadista cobró

relevancia —fue la única que investigó la policía desde el principio— y fue admitida por las autoridades. El 3 de abril los autores materiales, islamistas, fueron aislados en un apartamento de Leganés, donde se suicidaron, llevándose consigo la vida de un miembro del Grupo Especial de Operaciones de la Policía Nacional. Al concluir la investigación y el juicio, en 2007, quedó indubitadamente probado que había sido un atentado inspirado por Al Qaeda y ejecutado por seguidores de esa red criminal.

Desde el primer momento, el diario *El Mundo* y algunos medios digitales de tendencias derechistas defendieron una teoría paralela que afirmaba que había sido obra de ETA con la colaboración de la policía, el CNI y la Audiencia Nacional para lograr un cambio de gobierno —las elecciones fueron ganadas por el PSOE cuando hasta entonces las encuestas daban mayoría al PP, en el poder— y, de esta manera, conseguir beneficios para la banda asesina o para la independencia de Euskadi. Para ello se apoyaban en hechos aislados que carecían de significado en el contexto global —como que apareciese en una furgoneta utilizada en el ataque una tarjeta de visita del Grupo Mondragón, o que se encontrase ácido bórico, un compuesto de venta libre que sirve para evitar el mal olor de los zapatos, en casa de un yihadista y también en posesión de algún etarra—. Algunos conspiranoicos llegaron a la bellaquería de afirmar que los miembros del GEO asesinaron a su compañero Francisco Javier Torronteras para encubrir la conspiración. Por ejemplo, en el blog *losrockefeller.wordpress.com*, donde se afirma que «le llevaron a morir y le dejaron morir» y «al GEO Torronteras lo llevaron al matadero».

En este caso concreto se dan todos los elementos que muestran la presencia de una teoría imaginaria. Gran número de gentes con intereses contrapuestos o hasta enemigos que se unen entre sí sin que nadie hable, un responsable en las sombras del que nada se sabe con certeza, la utilización de elementos aislados ciertos para llegar a conclusiones disparatadas y, por supuesto, la falta de formación de sus defensores, incluidos los llamados *peones negros*, nombre que se dieron a sí mismos los conspiranoicos, entre los que se decía que había policías y periodistas. La peculiaridad respecto a otras teorías es que esta recibió apoyo de ciertos medios y hasta comprensión por parte del principal partido de la oposición, como forma de desgaste al gobierno de Rodríguez Zapatero. Las conspiraciones ficticias suelen tener su nicho editorial en libros marginales de nula credibilidad, pero es muy extraña su aparición en la prensa seria, porque se desacredita a sí misma dándoles pábulo. Cuando los intereses electorales cambiaron, también decayó la atención en la prensa más próxima al PP y, con el paso del tiempo, ha quedado relegada al grupúsculo de irreductibles habituales de las redes sociales, los mismos que abrazan otras elucubraciones similares.

Aunque hemos mencionado algunas mentiras que gozan de credibilidad en Internet, algunas inocentes y otras que bordean la criminalidad, hay muchas más, puesto que en la Red hay tribuna libre y cualquiera puede escribir lo que le plazca. Es responsabilidad del internauta concienciado no fiarse de algo solo porque esté escrito

y verificar siempre las fuentes y su credibilidad.

10

LOS GOBIERNOS DEL SILENCIO

En 2010, en Egipto gobernaba el dictador Hosni Mubarak, que reprimía con mano de hierro a la oposición y a los ciudadanos que hablaban de más. Una de las obsesiones del régimen era el control de Internet. Si una imagen en que se viera la corrupción imperante llegaba a la Red, su difusión podría ser imparable, por lo que las autoridades se amparaban en una cuasi ilegal Ley de Emergencia para proceder a la identificación, en cualquier momento, de todos los que estuvieran en cualquier lugar público —como un locutorio— y, a continuación, revisar su actividad en el ordenador que estuvieran usando. Era norma detener a los blogueros, golpearlos con saña y mantenerlos bajo arresto hasta que las marcas se desvanecían. Así buscaban acallar las críticas al poder, dado que prohibir Internet, una de las principales distracciones de la juventud, podría producir el efecto contrario al deseado e instigar una revuelta.

El 6 de junio, un chaval de veintiocho años llamado Jaled Mohamed Saeed estaba en un cibercafé del distrito de Sidi Gaber, muy cerca de su casa, en la norteña ciudad de Alejandría. Hacía un tiempo había subido a la Red un vídeo que fue bastante popular en el país y despertó un odio especial contra el chico por parte de los implicados. En él se veía a varios policías repartiéndose los beneficios tras una operación contra el tráfico de drogas.

Aquella infausta tarde llegaron al establecimiento dos agentes de paisano y pidieron la documentación de todos los presentes. Saeed ya sabía que no despertaba simpatías entre la corporación, de cuya brutalidad nadie tenía dudas. Pensó que su mejor opción era negarse a la identificación, puesto que si averiguaban su nombre, sería peor. Gesto inútil, porque los oficiales eran conscientes desde el principio de a quién tenían delante y esa fue la excusa que necesitaban. Le esposaron las manos a la espalda, pero, en vez de llevárselo al vehículo policial, comenzaron a golpearlo allí mismo, delante de todo el mundo. Estrellaron su cabeza contra el suelo de mármol y luego lo arrastraron fuera del edificio, donde continuaron la paliza. Ya estaba cubierto de sangre cuando los transeúntes comenzaron a rogarles que se detuviesen. Incluso dos médicos presentes intentaron ayudar, sin suerte. Le golpearon el cráneo contra una puerta de hierro y contra los escalones de una casa cercana. Más policías comenzaron a llegar ante la cantidad de testigos que se estaban arremolinando y acordonaron la zona. Al chico lo arrojaron en un coche de la institución y abandonaron la zona. Los policías recién llegados, por su parte, confiscaron todos los teléfonos móviles de los presentes y cualquier otro dispositivo de grabación donde pudiera haber pruebas de lo que acababa de pasar.

Quince minutos más tarde, el cadáver desfigurado de Jaled apareció tirado en

una cuneta, dentro aún de la ciudad.

Lo que podría haber sido un caso más de la impunidad en países dictatoriales creció en las redes. La autopsia determinó que había fallecido por ingerir un alijo de hachís al reparar en la presencia policial. Su hermano, al acudir a identificar el cadáver, le hizo subrepticiamente varias fotos que corrieron por Internet como la prueba irrefutable de la mentira: un rostro destrozado, con la mandíbula rota por varios sitios, el cráneo fracturado, golpes y arañazos por todos los lados y sangre que manaba de los oídos y la boca.

Wael Ghonim, un egipcio residente en los Emiratos Árabes Unidos, ejecutivo de Google y activista de Internet, creó la página web, dentro de Facebook, Todos somos Jaled Said, que atrajo a cientos de miles de compatriotas hasta convertirse en el sitio opuesto al régimen más popular del país. Tanta fue su influencia que consiguió que los dos responsables de la paliza fueran entregados a la justicia. Recayó sobre cada uno de ellos una sentencia de diez años por homicidio.

El gobierno de Mubarak había reaccionado tarde y mal. A pesar de que el 27 de enero de 2011 Ghonim fue detenido y el acceso a Internet suspendido en todo el país durante doce días, la bola de nieve era demasiado grande y, junto con la influencia de la Revolución de los Jazmines que había estallado en Túnez, el pueblo se echó a la calle. El dictador tenía contadas las horas en el poder.

CUANDO HABLAR ES DELITO

Una de las obsesiones de los regímenes autoritarios es el control de la información. Los medios de comunicación de masas pueden influir en la población lo suficiente para causar su derrocamiento. Parte del éxito de un dictador consiste en tener a la población convencida de que es necesaria su presencia o, por lo menos, mantenerla apaciguada, porque ni el más poderoso de los ejércitos puede controlar a un pueblo cuya mayoría esté enfurecida. Las fuerzas armadas están formadas por personas de ese mismo país y, como tales, son susceptibles de ser influidas también. Así, una de las primeras formas de detectar una deriva autoritaria es la prohibición de la prensa no afín. En España el control de las publicaciones estuvo presente durante toda la dictadura de Franco y hasta, por lo menos, el real decreto-ley 24/1977 de 1 de abril. Hoy, el secuestro de números solo puede hacerse bajo las órdenes de un juez. Hasta entonces, la Administración lo ejecutaba ante cualquier obra contraria a los Principios Fundamentales del Movimiento o tan solo molesta para el gobierno.

La llegada de Internet ha causado una revolución sin precedentes en las comunicaciones, con una velocidad sorprendente: las posibilidades aparecen y se multiplican mucho más rápido que la legislación que pueda regularlas. Esto es peligroso para los totalitarismos por dos motivos. Por un lado, los disidentes no necesitan reuniones personales o utilizar vulnerables teléfonos para llamarse. Hoy

pueden comunicarse por mensajería electrónica, chats o foros ubicados en la red TOR, tanto públicos como privados y no tienen por qué verse las caras jamás. A menudo no pueden dar información sobre la naturaleza de los otros *miembros* de su *organización*, más allá del apodo que utilizan, porque nada más saben. Este bajo riesgo y la comodidad de acceso, provocan la activación de una mayor cantidad de opositores. Antes de Internet, bien por miedo, bien por el excesivo esfuerzo necesario, los ciudadanos no *se metían en política*. Los que daban el paso tenían que acudir a asambleas clandestinas o repartir de tapadillo pasquines o panfletos impresos. Ahora cualquiera puede opinar y su opinión puede tener un gran eco.

Por otro lado, la prensa tradicional, aquellos diarios, radios o televisiones destinados a llegar a una gran cantidad de gente, pueden ser alojados en Internet más allá del alcance censor. Medios opositores siempre han existido, pero su difusión era menor y más comprometida. En España fue importante desde 1941 Radio España Independiente, conocida como La Pirenaica, aunque emitía desde Rusia primero y Rumanía después. Estaba organizada por el Partido Comunista de España en el exilio y fue un quebradero de cabeza para el franquismo, que intentó silenciarla o interferirla con técnicas diversas. Con las capacidades actuales, basta teclear en el navegador para acceder a los periódicos oficiales de cualquier *enemigo del país*, y con una censura mucho más difícil.

Ante este riesgo muy cierto, los países sin libertad han actuado de formas diferentes. Por un lado, está el más drástico, Corea del Norte, que tiene prohibido el acceso a la Red, salvo para el tres por mil de su gente, los más altos funcionarios del régimen. Las zonas rurales y hasta varias ciudades carecen incluso de electricidad, mucho menos de ordenadores y, de hecho, solo existe un cibercafé y está en la capital, Pyongyang. Usan un sistema operativo propio, Estrella Roja, y solo pueden acceder a su propia Intranet, llamada *Kwangmyong*, con la que se pueden consultar portales de noticias propiedad del régimen. Para la interacción ciudadana hay foros y chats internos donde todos están identificados. Incluso un pequeño error ortográfico puede acabar con el redactor de un medio digital y toda su familia en un *centro de reeducación*, eufemismo para los famosos campos de concentración con altísimos porcentajes de fallecimiento. La mera tenencia de un teléfono móvil conduce al mismo destino. Kim Jong-un está invirtiendo en tecnología con la que detectar esas llamadas o el uso de datos, y son habituales los rastreos policiales de usuarios. Esos *smartphones* provienen de contrabando de la vecina y aliada China y funcionan hasta a diez kilómetros de la frontera, utilizando las redes de aquel país. El propósito es claro: si nadie puede tener acceso a Internet, no habrá problemas de subversión.

Otro caso paradigmático es el de Cuba, país que la ONG Reporteros sin Fronteras considera «enemigo de Internet» desde el año 2006. Allí los problemas se acumulan. El largo bloqueo al que está sometida por parte de Estados Unidos ha impedido una conexión normal, a pesar de tener, a solo treinta y dos kilómetros al norte de sus costas, una de las más tupidas redes de telecomunicaciones, los cables oceánicos de

Florida. Para remediarlo, en 2007 se firmó un contrato con la Venezuela de Hugo Chávez por el que se tendería un cable submarino de mil seiscientos kilómetros, que estuvo acabado en 2011 y empezó a funcionar dos años después. Hasta ese día, la conexión en la isla era vía satélite y lenta hasta la exasperación. Estaba limitada a ciertas profesiones, como militares, funcionarios de agencias gubernamentales y, sobre todo, médicos, restringida a dominios cubanos y a ciertas páginas relacionadas con su actividad. Desde entonces, el gobierno, a través de la empresa gubernamental ETECSA, ha ido construyendo puntos de acceso inalámbrico en las plazas de las ciudades, que llegaron a ochenta y cinco en 2016, con las que consigue acceder a la Red el cinco por ciento de la población mediante la compra de tarjetas con contraseñas. Su precio es exorbitante, dos pesos cubanos convertibles por hora —tres si se compra a vendedores ambulantes—, cuando el sueldo medio en esa misma moneda es de veintitrés al mes. Esta es otra forma de limitación del acceso al servicio, dado que muchos no se lo pueden permitir. Además, al ser en lugares públicos, la posibilidad de un uso subversivo de Internet es todavía más difícil, porque las pantallas pueden ser espiadas por los presentes y distinguir la actividad de quien está en un lugar concreto es fácil con herramientas informáticas adecuadas.

Después de acceder con una velocidad de caracol, muy lejos de los estándares europeos, la férrea censura bloquea muchas páginas. En otros casos, las compañías estadounidenses no están autorizadas a trabajar en la isla. El servicio de videollamadas Skype, uno de los más populares, está vetado. Los cubanos, habituados a encontrar soluciones a todo, utilizan Imo, con funcionalidades parecidas. La plataforma de compra-venta Craiglist, muy popular en su gran vecino del norte aunque desconocida en España, es sustituida por la local Revolico, que hasta tiene un interfaz muy similar. Dada la imposibilidad de descargarse películas o series de televisión —ni hablar de verlas en *streaming*—, estas entran en el conocido como *paquete semanal*, un disco duro clandestino con los estrenos audiovisuales que pasa de mano en mano, copiándose en todos los dispositivos de la isla.

Los expertos en la censura de Internet son los chinos. Con un quinto de la población mundial bajo el dominio de una dictadura comunista con economía de mercado, es necesario un delicado equilibrio entre el ocio y los negocios. Hay que evitar el uso de la herramienta contra el régimen.

La red sirve para comerciar con menos intermediarios. Una página web alojada en aquel país y manejada por sus ciudadanos puede colocar sus productos en el destinatario final de cualquier lugar del mundo con muchos menos costes y de manera más efectiva. En el portal de subastas y venta *online* eBay muchas tiendas virtuales están radicadas en aquel país o bien son distribuidores de aquellas en Europa. El sitio paradigmático de comercio chino es el conglomerado Alibaba, fundado en 1999 por el empresario y filántropo Ma Yun (conocido en occidente como Jack Ma). Una de sus páginas, Aliexpress, está pensada para el consumidor final, mientras que otras, como la que da nombre al grupo empresarial, se utilizan para

relaciones entre productores y mayoristas. Solo en 2012, Alibaba movió ciento setenta mil millones de dólares.

Ya hemos visto en capítulos anteriores cómo es utilizada Internet para proporcionar otro tipo de servicios, como la generación, tanto legal como ilegal, de bienes en los juegos *online*. A cambio, buena parte de la publicidad no deseada que inunda los correos electrónicos proviene de allí; en 2004 se calculó que hasta el setenta y uno por ciento del total, si bien desde entonces se ha redistribuido.

El control de la Red lo llevan a cabo mediante una gigantesca trama de cortafuegos, cuyo principal elemento recibe el nombre oficial de *Proyecto Escudo Dorado*, que empezó a construirse en 1998 y a funcionar en 2003. Completó su cobertura tres años más tarde. Es una paradoja que la mayor parte de los equipos informáticos y electrónicos necesarios hayan sido proporcionados por empresas de Estados Unidos, que afirma ser el defensor de la libertad individual. El principal objetivo es bloquear páginas web que vayan contra los principios de la Revolución. Para ello usan varios métodos, entre ellos el filtrado de IP, que hace que todas las peticiones de los ordenadores chinos pasen a través de los *proxies* del Proyecto, que comprueban si aquella en la que se ubica determinada página web —recordemos el capítulo uno— está en la lista prohibida y, en ese caso, rechazan todas las peticiones que se realizan desde China a esa dirección concreta. Otras formas de evitar que lleguen los contenidos es el filtrado de paquetes TCP/IP. En esta modalidad, los sistemas los analizan de uno en uno, buscando palabras significantes de subversión y, si las hallan, lo destruyen y terminan con la conexión de quien las ha emitido. Los bloqueos van cambiando con el tiempo. Lugares donde domina la opinión, como muchos sitios de blogs personales entre los que destacan Wordpress o Blogger, son prohibidos de forma intermitente. Servicios de correo electrónico internacional como Gmail también sufren cortes. Incluso si se realiza en China una búsqueda desde Google de sucesos o lugares significativos, sus resultados difieren de lo que se encuentra en Europa o Estados Unidos. La búsqueda de la palabra *Tienanmen*, la plaza de Pekín donde hubo una protesta popular de estudiantes en 1989, reprimida con dureza por el Ejército, que causó cientos de muertos y miles de heridos, lleva aquí a la icónica fotografía de un hombre, desarmado, bloqueando con valentía una columna de carros de combate. En el país asiático, por el contrario, solo conduce a imágenes de la plaza vacía o durante celebraciones populares.

Para evitar estos cortes intermitentes con las webs internacionales, gran parte de la actividad se lleva a cabo dentro del país. En vez de Google, usan Baidu. En lugar de YouTube, Yogoo. En esos sitios, además, la información es controlada con mayor facilidad por el Estado, que puede eliminar o modificar contenidos a voluntad.

Muchos ciudadanos piensan que espían de forma directa sus comunicaciones —esto es, que todos los correos o mensajes de chat son supervisados uno a uno, algo imposible de llevar a la práctica—, lo que hace que se impongan una autocensura muy beneficiosa para el gobierno, que refuerza esa sensación con propaganda y

medidas legales. En el país, los proveedores de servicios pueden ser acusados de lo que hagan quienes los utilizan. Eso quiere decir que si en una web local que proporciona alojamiento gratuito se aloja un comentario crítico al gobierno, la empresa es tan responsable como quien lo ha colgado allí.

China no duda en encarcelar a opositores que utilicen la Red. Algunos incluso no son muy conscientes de estar siendo subversivos. El 12 de mayo de 2008 hubo un terremoto en la provincia de Sichuan que causó casi setenta mil muertos. Lui Shaokun era maestro en una escuela de la zona e hizo fotografías a los colegios, que, debido a una construcción defectuosa, habían colapsado con facilidad, atrapando a multitud de niños. Luego las subió a Internet para denunciar lo que él entendía que era una trama corrupta que debía ser investigada. No culpaba al gobierno ni a las instituciones, sino que les suplicaba ayuda. Fue detenido el 25 de junio, acusado de «esparcir rumores y dañar el orden público» y recibió una sentencia administrativa —contra la que no cabe apelación ni recurso— de «un año de reeducación a través de trabajos forzados». No fue el único que cumplió cárcel por el mismo hecho. Huang Qi, un conocido activista por los derechos humanos de la misma zona, fue a prisión por «posesión ilegal de secretos de Estado» tras publicar artículos en los que se explicaban los fallos estructurales de los centros docentes. Estos dos ejemplos son una gota en el océano de la represión en aquel país.

La situación es parecida en otros lugares. En el mundo islámico en especial, la censura de Internet y el control de los disidentes son extensos. En Irán, otro de los países nombrado «enemigo de Internet», la mitad de los quinientos sitios más visitados en el mundo están vetados, incluyendo Facebook, Twitter, YouTube o Google Plus. Es decir, todos aquellos susceptibles de alojar opiniones y que, por tanto, pudieran ser perjudiciales para el régimen. No son los únicos. Según la página *ViewDNS.info*, que monitoriza la actividad de Internet, hasta el noventa y siete por ciento de las páginas para adultos son inaccesibles, como casi el veinte por ciento de las de negocios y las infantiles, un tercio de las informativas y un cuarto de las dedicadas a juegos o a ordenadores. También hay una tradición represora y encarceladora de los blogueros rebeldes o hasta de los técnicos instaladores. Todo eso en un país con más de cuarenta y seis millones de internautas, casi siete de cada diez habitantes.

Las comunicaciones se innovan a mayor velocidad que las formas de combatirlas. Una vez que se tiene la posibilidad técnica de acceder, casi siempre hay opciones de burlar el bloqueo. Por eso, el método coreano es el único seguro, al impedir su uso por los ciudadanos, salvo excepciones muy restringidas. En Cuba ya hemos visto cómo están acostumbrados a encontrar alternativas. Si una forma de comunicación no funciona, se busca otra. Ese pensamiento lateral es el que sirve, a mayor escala, para superar la censura. Si las formas de conexión habituales no funcionan o están supervisadas, habrá que encontrar unas que no lo estén. Una de las más sencillas, muy popular en China y válida en casi todos los demás países, es el uso de *redes*

privadas virtuales, VPN por sus siglas en inglés. Este método conecta un ordenador de cualquier lugar del mundo, a través de un *túnel*, con una red local ubicada en otro país, con lo que se navega a casi todos los efectos como si se estuviera en aquel lugar. De ahí su nombre, puesto que usa Internet para acceder a una red local a la que, en puridad, no pertenece. Los estudiantes españoles en aquel país suelen hacerlo con la universidad del lugar del que proceden, y así, por lo menos, pueden acceder a sus correos electrónicos y, con suerte, a sus redes sociales en los momentos en que están cerradas en la Internet pública. Para crear ese túnel, es necesario tener un usuario y contraseña con los que autenticarse en el otro lado. Todos los paquetes TCP/IP que se envíen y reciban van cifrados de origen a destino, con lo que incluso los sistemas que espían el interior de su contenido no sabrían lo que poseen. La principal desventaja es la lentitud de la conexión, que, en el mejor de los casos, será tan rápida como el canal más lento utilizado, entre principio, fin y camino. Las autoridades no estaban muy contentas con este agujero, así que desde 2011 empezaron a utilizar métodos para bloquear las VPN más conocidas, con éxito variable. Los más expertos aprendieron a camuflar —ofuscar, en un desafortunado anglicismo utilizado en seguridad informática— sus paquetes TCP/IP, de forma que no parezcan ser de una red privada virtual.

Desde China, como en la mayor parte de los países censores, no se puede acceder tampoco al lugar oficial desde el que se descargan los programas que permiten acceder a TOR. Esta prohibición también puede saltarse con facilidad —por ejemplo, buscándolo en una red de descarga directa o utilizando protocolos encriptados para ir al sitio original—. Una vez instalado, la navegación tampoco es fácil. El Escudo Dorado bloquea casi todos los tres mil nodos más habituales de esa *deep web*, de manera que es muy difícil enviar paquetes y que vuelva la respuesta. El proyecto TOR, según informa en su propia página, tiene prevista una serie de puntos secretos, llamados *puentes*, para ayudar a países con ese tipo de denegación. La principal diferencia respecto a los normales es que no existe en ningún lugar una lista completa y van variando con el tiempo. Los operarios gubernamentales realizan continuas búsquedas, pero van siempre un paso por detrás —dado que no pueden encontrar algo hasta que no lleve un tiempo funcionando—. Por si eso fuera poco, el sistema permite activar lo que denominan *transportes conectables —pluggable transports* en inglés —, que camufla los paquetes que envía y recibe TOR como si no fueran suyos, de manera que los sistemas de detección automáticos no encuentran motivos para pararlos.

También existen programas dedicados en exclusiva a rodear los bloqueos que establecen los países. Uno de los más conocidos es *Psiphon*, creado en Toronto (Canadá) y durante un tiempo mantenido por la universidad de aquella ciudad antes de establecerse como empresa independiente. Consiste en una serie de protocolos combinados que dan una buena posibilidad de superar los filtros. Todos estos medios de evitar la censura tienen un mismo problema: si la policía detecta suficientes

conexiones *sospechosas*, puede realizar un registro en el domicilio en el que encontraría las pruebas de lo que hacen. Por eso es más seguro que los disidentes utilicen conexiones que no sean la propia, bien mediante el uso de tarjetas telefónicas sin titular identificado, bien mediante conexiones inalámbricas o cibercentros, cuando eso sea posible.

Según la ONG estadounidense Freedom House, dedicada a promocionar la libertad política, la democracia y los derechos humanos, los países donde Internet está más restringida son Cuba, Gambia, Bielorrusia, Rusia, Kazajistán, Uzbekistán, China, Siria, Irán, Pakistán, Emiratos Árabes Unidos, Bahréin, Arabia Saudí, Egipto, Sudán, Etiopía, Myanmar, Tailandia y Vietnam. Además, carecen de datos sobre Corea del Norte y la mayor parte de África.

EL MUNDO ÁRABE ROMPE SU AISLAMIENTO

Los países árabes se extienden desde Marruecos por el oeste hasta Omán por el este. Su territorio incluye la franja sur del Mediterráneo, Oriente Medio —salvo Israel y un Líbano donde los cristianos tienen mucho peso— y la península arábiga. Hay otras naciones musulmanas de otras etnias. Turquía, Irán y el país con más fieles del mundo, Indonesia, son ejemplos de estos últimos. El Islam es una religión que abarca todos los aspectos de la vida, mucho más allá de la espiritualidad, desde la política a la personal, e incluso define los hábitos de higiene. No existe el concepto de *democracia* en su acervo, porque era ajena a la realidad de Mahoma en Arabia cuando redactó el Corán. Los gobiernos han sido autoritarios, de la teocracia al dictador de partido único, pasando por las monarquías de inspiración divina. Los conflictos internos se han debido a otro tipo de tensiones, en especial entre diversas creencias o ramas de la misma religión. Según una encuesta realizada a treinta y ocho mil musulmanes suníes —la facción mayoritaria— por el Centro de Estudios Estratégicos de Estados Unidos, más de la mitad de ellos cree que los chiíes —el grupo minoritario, fuerte en Irán— no profesan su misma religión.

En 2016, tras la Revolución de los Jazmines que veremos a continuación, solo Túnez puede considerarse un país democrático, mientras que Marruecos, Argelia, Egipto, Sudán, Kuwait y Jordania tienen una democracia restringida o parcial. Mauritania, Arabia Saudí, Bahréin, Qatar, Omán y los Emiratos Árabes Unidos son dictaduras, bien militares, bien teocráticas. Libia, Siria, Iraq y Yemen están envueltos en guerras civiles, en los dos primeros casos como resultado directo de la llamada Primavera Árabe y sus consecuencias posteriores.

Una vasta población, hasta cuatrocientos cincuenta millones de habitantes, ha vivido en un tradicional aislamiento debido al control de los medios ejercido por los estados. Solo se informaba desde la perspectiva que interesaba a cada régimen y se ocultaban hechos a conveniencia. La penetración de Internet fue progresiva, pero

muy importante. Los gobiernos no supieron ver al principio el potencial de la Red, no lo temieron como para prohibirlo, lo que luego traería consecuencias. Como ya hemos visto, la única forma real de evitar que la población la utilice es bloquear la señal en el país. Si hay Internet, hay maneras de evitar la censura. No obstante, un sistema restrictivo con suficiente eficiencia disuade a la mayoría, evitando así una masa crítica que pueda iniciar una revolución o protestas generales.

Los jóvenes, más inclinados a la utilización de nuevas tecnologías, gracias a Internet consiguieron, en primer lugar, acceso a información de otros lugares del mundo. Comprobaron que existían otras sociedades y otras formas de gobierno y empezaron a pensar «¿Por qué no nosotros?». La influencia cultural occidental fue más intensa gracias a las películas, la televisión y elementos de ocio sin censurar que se descargaban, que por motivaciones políticas tradicionales. El segundo papel principal lo jugó la prensa extranjera, donde se podían formar opiniones basadas en puntos de vista prohibidos por los regímenes. El depósito estaba lleno de gasolina y solo hacía falta la chispa que la prendiera. Fueron varias. La primera, en Túnez.

Desde 1987, el dictador Ben Alí gobernaba el pequeño país de poco más de diez millones de habitantes, apoyado por Estados Unidos y por la antigua metrópoli, Francia. Había sucedido al anterior presidente, el primero desde la independencia treinta años antes, y de la misma naturaleza totalitaria. El cuerpo jurídico y social del sistema se caracterizaba por el favorecimiento del capital extranjero, que poseía numerosos hoteles y negocios turísticos, y por su moderación religiosa. Fue la primera nación norteafricana en prohibir la poligamia y los tribunales tradicionales o *habous*. Las universidades y escuelas coránicas estaban bajo el control directo del Ministerio de Educación. Más aún, las mujeres gozaban de unos derechos no vistos en el resto del mundo islámico. En 2009 el Foro Económico Mundial consideró su economía como la más competitiva de toda África. El desempleo rondaba el quince por ciento. Por otro lado, su partido ganaba casi el cien por cien de los escaños en cada ocasión y sujetaba a los medios con mano de hierro. El Estado concedía las licencias preceptivas para prensa escrita o radio, que podían ser revocadas. No autorizaba a las que podían ser críticas con su labor. Otra forma de presión era el control de publicidad institucional, que solo era concedida a los medios afines o, al menos, dóciles. La legislación prohibía ofender al presidente del país, alterar el orden público o difundir noticias falsas —desde el prisma gubernamental— lo que, en la práctica, representaba la imposibilidad de contar todo lo que resultase molesto a las autoridades.

La vigilancia de Internet era exhaustiva. El país también estaba en la lista negra de Reporteros Sin Fronteras, que lo consideraba en 2009 el más autoritario de la región por la persecución de libertades civiles. Al mismo tiempo, era el que tenía precios más bajos de toda África para acceder a la Red y con una penetración en la población de cerca del treinta y cinco por ciento, superior a la media mundial y mucho mayor que la africana, que apenas superaba el once. Según informa la

Iniciativa Red Abierta —OpenNet Initiative, una organización canadiense contra la censura en Internet—, muchas páginas web estaban vetadas, entre ellas las de todos los partidos de la oposición y de organizaciones de defensa de los derechos humanos, como las dos ONG que hemos nombrado en este capítulo, Amnistía Internacional y hasta la Comisión Islámica de Derechos Humanos. Las páginas de descarga de anonimizadores de conexión como TOR también estaban bloqueadas, aunque conseguir el programa por otros medios, como en el caso chino, era relativamente fácil. De hecho, el tráfico en la *deep web* se incrementó de forma acusada durante las revueltas. Como es tradicional en naciones musulmanas, toda la pornografía y páginas de citas para homosexuales estaban prohibidas. Más llamativo, Facebook también estaba entre las páginas inalcanzables hasta que fue liberado por una orden presidencial, sin dar más explicaciones. En 2010 se bloqueó el protocolo SIP, el utilizado para videoconferencias a través de Skype, que era utilizado en muchos locutorios para las llamadas internacionales. Como consecuencia, se perdieron muchos puestos de trabajo, lo que se sumó a una crisis ya acuciante en el país.

De ese control exhaustivo no se salvaban ni servicios en principio privados. OpenNet realizó un experimento en que el activista tunecino Sami Ben Gharbia, que residía en Holanda en esa época, recibió las credenciales para los correos electrónicos de dos colegas suyos que estaban en el país africano y, con su permiso, accedió a ellos. Comprobó que desde Europa se veían mensajes que no aparecían al otro lado del Mediterráneo. Así se demostró que la censura automática llegaba incluso a violar el secreto de las comunicaciones, para lo que se amparaban en una ley de 1998.

Los opositores eran perseguidos de manera sistemática. En 2005, el activista tunecino por los derechos humanos Mohammed Abbou fue condenado a tres años y medio de cárcel por publicar un informe en Internet donde se hablaba de la tortura de la que eran víctimas los detenidos bajo el régimen.

Wikileaks, de la que hablaremos a continuación, había enviado en el último tercio de 2010 miles de documentos al diario *El País* —único español entre otros extranjeros— en los que se hablaba de un Túnez enfermo por la corrupción y en que la familia de Ben Alí era una suerte de mafia que incluso falsificaba documentos a voluntad. El embajador de Estados Unidos hasta 2009, Robert Godec, afirmaba en cables dirigidos a sus jefes y filtrados por el mismo medio que el dictador estaba anciano, debilitado por el cáncer y que se pasaba el día jugando con su hijo de cinco años. Describía a su esposa, Leila, como ansiosa de poder y verdadera gobernante que pensaba que iba a heredar el cargo; su marido cumplía todas sus voluntades. Explicaba que el país estaba corrupto hasta la médula, lo que indignaba a la población, junto a las desigualdades regionales y el desempleo.

En este contexto, el 16 de diciembre de 2010, en la ciudad de Sidi Bouzid, la policía confiscó el carrito de venta ambulante de un joven universitario en paro, Mohammed Bouazizi. Algunas fuentes afirman que fue porque no había podido pagar el soborno acostumbrado. Condenado a la miseria, se roció de gasolina frente a la

Prefectura de Policía y se prendió fuego. Falleció por las graves heridas el 4 de enero del año siguiente. Fue el principio de lo que se conoció desde fuera como Revolución de los Jazmines y en el interior como Revolución de la Dignidad.

La noticia de la inmolación corrió como la pólvora y esa misma tarde comenzaron las primeras manifestaciones en la ciudad. Fueron reprimidas con extrema dureza, lo que causó que al día siguiente las protestas derivasen en actos vandálicos. El gobierno dio instrucciones a la prensa de no hablar sobre ello, pero no pudo evitar que en Facebook y YouTube se pudieran ver informaciones sobre lo que estaba ocurriendo que alentaron y esparcieron el alcance del levantamiento civil a otros puntos del país. A finales de diciembre, otros dos ciudadanos, *inspirados* por Bouazizi, se habían suicidado como forma de protesta por su precaria situación, a lo que hay que sumar otros dos muertos y múltiples heridos causados por la represión policial. El régimen se asustaba y buscaba la cabeza de un movimiento que no la tenía, convocado a través de las redes sociales de forma casi espontánea. Como las canciones del rapero local conocido como *El General*, Hamada Ben Amor, eran utilizadas como himno de la revolución, fue detenido, aunque puesto en libertad poco después, dado que el hecho causó una escalada en las protestas. También desaparecieron o estuvieron bajo arresto seis blogueros, incluido Slim Amamou, que más tarde fue secretario de Estado de Juventud en el gobierno de transición que siguió a la caída de Ben Alí.

El siguiente intento fue el control de la Red. Por un lado, bloquearon más páginas web de las habituales, incluida Wikileaks, en un intento por cortar el flujo de información. Después fueron un paso más allá. Todo el tráfico de Internet del país pasaba por la empresa pública de telecomunicaciones ATI, por lo que quien tuviera acceso a ella tendría un control casi absoluto sobre la navegación, no solo para espiar lo que se hacía, sino para manipularlo. Se aprovecharon de ello y, cuando cualquier ciudadano intentaba acceder a las redes sociales, en especial Facebook, se encontraba con la habitual petición de usuario y contraseña en una página idéntica, salvo que quien se lo pedía no era la empresa legítima, sino que los datos eran volcados a un servidor y después el ordenador era redirigido a la verdadera web. Era un *script* o reducido programa fácil de hacer y que es habitual encontrar en pequeños delincuentes informáticos por todo el mundo. Desconocidos, aunque sin duda de parte del gobierno de Ben Alí y probablemente de sus servicios secretos, recopilaban toda esa información, con lo que podían hacerse pasar por cualquier usuario que hubiera entrado al sitio web desde el país. Y, de hecho, lo hacían. Así pudieron empezar a borrar páginas contra el gobierno, aquellas donde se organizaban las manifestaciones o las propias cuentas de los opositores, intentando evitar que las protestas crecieran y salieran del ámbito regional. Pero ya era inútil. Demasiada gente tenía conocimiento de ellas y se comunicaba por diversos medios. Se extendieron por diversas áreas del país, incluyendo la capital, y las élites comenzaron a apoyarlas. Los primeros, los abogados, que iniciaron una huelga el 6 de enero. Las Fuerzas Armadas

les siguieron, desde los más altos mandos hasta las clases de tropa. En Túnez, al contrario que en otros países árabes, los generales no tenían intereses económicos de gran magnitud que pudieran perder con un cambio de régimen. El 14 del mismo mes, Ben Alí y su familia huyeron del país con destino Arabia Saudí. Su situación era insostenible. Los militares habían expulsado a la Guardia Presidencial y tomado el palacio. Las otras opciones para Alí eran la prisión o la muerte.

Las protestas no cesaron de inmediato. La población era recelosa del gobierno de transición e incluso hubo un intento poco exitoso de establecer un califato islámico por parte de una organización internacional. Sin embargo, con entradas y salidas del gabinete y otros altibajos, la nación caminó hacia una democratización extraña en el norte de África, aun con los defectos de quien está empezando ese camino. Reporteros sin Fronteras le retiró el título de enemigo de Internet para ponerlo en el apartado «bajo vigilancia».

El éxito de las protestas fue uno de los incentivos que contagió la revolución a Egipto, entre otros. El dictador Mubarak había tomado buena nota de lo ocurrido y fue más drástico, cortó Internet en el país tan pronto como el 27 de enero, con Ben Alí todavía en el poder. El efecto fue el contrario al esperado, un mayor levantamiento civil, lo que obligó a devolver una conexión muy censurada, pero aun así, efectiva. La penetración de la Red en el país del Nilo era muy inferior a la tunecina, con menos del veinte por ciento de la población alcanzada, y se limitaba sobre todo en las ciudades. Allí, el acceso a los cibercentros permitía que muchos jóvenes que no tenían conexión en su casa pudieran utilizar la Red. De hecho, la tortura y asesinato de uno de estos en un local de Alejandría fue la chispa que inició las revueltas que concluyeron con el derrocamiento del presidente, otras dos revoluciones, cambios de gobierno y una penetración del islamismo radical, que ha sido una constante en la zona y de la que Túnez ha sido una honrosa excepción, a pesar de los dos atentados contra turistas que costaron la vida a más de sesenta y tres personas en el año 2015.

China tomó buena nota de toda la Primavera Árabe y censuró todas las noticias de cada uno de los países implicados. Sabían lo peligroso que es el contagio de los levantamientos populares y el efecto que Internet puede tener en ellos.

ESTADOS UNIDOS TAMBIÉN TIENE MIEDO

El 4 de octubre de 2006 se registró el dominio *wikileaks.org*. En diciembre de aquel año ya publicó su primer documento, uno de muchos que pondría en lugares incómodos a los gobiernos occidentes, en especial al país más poderoso del mundo, los Estados Unidos de América.

Su servidor principal está alojado en un antiguo búnker nuclear en Suecia, en las instalaciones de la empresa PRQ, conocida por no hacer preguntas sobre sus clientes

y no mantener un registro de actividad sobre quién accede a sus servicios. El país fue elegido, además, porque su Constitución prohíbe preguntar sobre las fuentes que utiliza cualquier noticiero. Hay copias de todo su contenido en otros países con protecciones legales similares y una más en un servidor oculto de la red TOR, cuya ubicación es desconocida. Así consiguen que sea casi imposible eliminar de Internet todo su contenido.

Se definen a sí mismos como una organización multinacional de prensa y una biblioteca asociada. Su fundador es el australiano Julian Assange, programador, editor y periodista. Aparte de él, los únicos nombres que se conocen del equipo directivo son los del islandés Kristinn Hrafnsson[3], Joseph Farrell y la británica Sarah Harrison[4]. El apartado legal está dirigido, desde 2012, por el exjuez de la Audiencia Nacional Baltasar Garzón en Europa y, en Estados Unidos, por el abogado Michael Ratner, presidente emérito del Centro para los Derechos Constitucionales. La empresa afirma tener en torno a cien trabajadores repartidos por los cinco continentes y que su mantenimiento económico proviene de su editorial, las ventas de sus publicaciones y la contribución del público en general. Disponen de una tienda virtual a la que se accede desde la web principal, en la que se vende desde ropa hasta tazas de desayuno, pasando por carcasas para móviles, paraguas o chapas con mensajes reivindicativos. Las camisetas están en torno a los treinta euros y una funda para iPhone vale veinte. Existe también un botón para emitir donaciones con una variedad de formas que incluyen tarjeta de crédito, cuentas de PayPal, transferencias bancarias, cheques o monedas virtuales como Bitcoin. Desde lo más moderno a lo más tradicional.

A pesar de su nombre y sus definiciones, Wikileaks no encaja con precisión con ninguna de ellas. WIKI significa, en inglés «lo que sé es…». Es un formato colaborativo para compartir conocimiento, cuyo máximo exponente es la celebérrima Wikipedia, una especie de enciclopedia del conocimiento universal, de lo más frívolo a lo más profundo, que está escrita y corregida por todo aquel que quiera participar. Hay cientos o miles de *wikipedistas* colaborando, por lo que crece y se actualiza más rápido de lo que podría hacer cualquier grupo reducido de expertos. Por contra, es vulnerable a borrados selectivos o a la introducción de información errónea, que podría permanecer tiempo hasta que algún lector o editor con conocimientos suficientes la detectase y enmendase. El proyecto de Assange no permite ese tipo de edición. Solo el personal que trabaja en la empresa puede editar y añadir nuevas entradas. Tampoco el interfaz gráfico es como las demás *wikis* que pueblan Internet. Es más parecido a un portal de noticias, con algunos buscadores que permiten, por ejemplo, rastrear por términos una base de datos formada por todos los correos intercambiados por el Partido Demócrata de los Estados Unidos. Solo una vez dentro de los artículos, la estructura guarda semejanza con Wikipedia.

Para ellos, WIKI hace referencia a que cualquiera puede aportar documentación que posea. Lo que cada uno sabe por estar en una posición privilegiada o que le ha

permitido tener acceso a datos secretos o clasificados. No funciona a base de rumores, sino de papeles auténticos, a menudo del gobierno de Estados Unidos. La organización garantiza el anonimato de las fuentes y verifica la autenticidad de los documentos antes de publicarlos o entregarlos íntegros a periódicos internacionales —en España suele ser *El País*—. Porque Wikileaks no es una biblioteca en la que se guarden libros o manuscritos, sino filtraciones, que es lo que significa «leaks» en inglés. Desde su fundación se ha dedicado a mostrar que los países más abiertos o libres también tienen un montón de cosas en su trastienda y han causado serios problemas diplomáticos.

Una de las quejas habituales es que están poniendo en riesgo a gente inocente, como víctimas de violaciones o aquellos perseguidos por su orientación sexual, debido a que publican de manera íntegra el material verificado. En 2016 colgaron datos sobre un saudí detenido por ser homosexual, algo que le puede costar la vida en su país, dado que se castiga con la pena capital. También han publicado la identificación de al menos dos víctimas de violación y de pacientes con problemas mentales. Han sido habituales las publicaciones de números de la Seguridad Social, teléfonos y tarjetas de crédito, datos que pueden ser utilizados por los delincuentes para cometer estafas o suplantaciones de identidad.

A pesar de estas quejas, la función de denuncia pública es innegable. Gracias a ellos hemos conocido verdades incómodas que de otra manera habrían quedado ocultas. Los primeros documentos que se pueden consultar en su amplia base de datos, fechados en 2007, se corresponden al equipamiento militar que utilizaba Estados Unidos en las guerras de Iraq y Afganistán. El salto a la fama ocurrió en 2010, con la publicación del vídeo *Asesinato colateral*. Son unas grabaciones de las cámaras que llevan instalados los helicópteros de ataque AH-64 Apache estadounidenses, que muestran una actuación en Iraq el 12 de julio de tres años antes. Se ve cómo disparan con fuego de cañón de treinta milímetros, pensado para destruir vehículos blindados, a una docena de personas, la mayoría de ellas desarmadas. Dos de ellos fueron identificados después como periodistas. También murieron o fueron alcanzados varios adultos y dos niños que intentaron rescatar a los heridos con una furgoneta. La agencia Reuters, para la que trabajaban los fallecidos, había intentado obtener esas imágenes en las que se ve que los militares en ningún momento estuvieron amenazados o en peligro. La investigación oficial anterior a su emisión, llevada a cabo por el Ejército de los Estados Unidos, concluyó en que se había actuado conforme a los protocolos establecidos, pero no entregaron la evidencia visual. El impacto en la opinión pública fue grande y ayudó a cambiar la forma de enfrentarse a la insurgencia en el país.

El siguiente gran hito de la web fue, aquel mismo año, la publicación de más de un cuarto de millón de telegramas intercambiados entre el gobierno del país norteamericano y doscientas setenta y cuatro de sus embajadas, desde 1966 hasta 2010. En ellos quedaban expuestas las políticas exteriores del país y su apoyo a

diferentes empresas privadas, a veces más allá de lo razonable. Sus revelaciones sobre el comportamiento de varios dirigentes árabes influyeron en la llegada de la Primavera apenas unos meses después. Otros se referían a las torturas de la base de Guantánamo. En lo que respecta a España, supimos cómo nos presionaron para cerrar las investigaciones judiciales de los «vuelos de la CIA», en los que sospechosos de terrorismo eran secuestrados en un país y trasladados a cárceles secretas en otros países. También había referencias la muerte del cámara de televisión José Couso por disparo de un carro de combate estadounidense en Iraq. Esos mismos cables revelaban que la vicepresidenta María Teresa Fernández de la Vega, el ministro de Asuntos Exteriores Miguel Ángel Moratinos, el fiscal general Cándido Conde-Pumpido y el juez de la Audiencia Nacional Javier Gómez Bermúdez habían ayudado de alguna manera a la expulsión de la carrera judicial de Baltasar Garzón.

Sin dejar de estar nunca de actualidad, el siguiente aldabonazo informativo lo consiguieron en 2016, cuando publicaron todos los correos que Hillary Clinton, secretaria de Estado durante la administración Obama, había intercambiado. Más de treinta mil mensajes, de los que ella había enviado siete mil quinientos setenta y el resto eran los recibidos. De nuevo quedaba expuesta la política del país y hasta la forma de comportarse de la candidata a la presidencia en las elecciones de ese año. Además, se pueden consultar muchos otros temas, desde actividades de multinacionales hasta datos sobre la economía global.

La actividad de Wikileaks ha expuesto a las personas conocidas y a la propia organización a represalias legales e ilegales. Tras el anuncio de que iban a publicar los telegramas diplomáticos, sufrieron un ataque masivo distribuido de denegación de servicio. Poco después, la empresa de alojamiento de dominios EveryDNS los eliminó de sus servicios, aunque ya había copias en muchos otros lugares, por lo que el efecto fue mínimo.

Después llegaron los intentos de asfixia económica. En primer lugar, Amazon retiró el sitio web de sus servidores tras las presiones de la administración Obama, para la que el hecho de que alojaran informes secretos era, como poco, de legalidad cuestionable. A los pocos días, PayPal eliminó la cuenta de la organización, seguida por Visa y Mastercard, de manera que los medios de financiación sufrieron un serio revés. El banco suizo PostFinance congeló los activos de Assange antes del fin del año. Hoy, las entregas de dinero a través de PayPal o tarjeta de crédito se hacen mediante intermediarios, las fundación Wau Holland y Por la Libertad de Prensa. Las monedas virtuales, por supuesto, siguen estando a nombre de la organización.

Estados Unidos ha perseguido con intensidad a los responsables de las filtraciones. En mayo de 2010 consiguieron detener al soldado Bradley Manning —hoy Chelsea, tras su cambio de sexo—. Asignado en Iraq como analista de inteligencia en 2009, aprovechó su posición para entregar a Wikileaks mucha información, entre la que destacan los ataques aéreos contra civiles y los telegramas diplomáticos. Entre los cargos estaban los de colaborar con el enemigo, lo que le

podía acarrear la pena de muerte. Se declaró culpable de diez acusaciones y el juicio, celebrado en 2013, le añadió otras siete más. La fiscalía quería una pena dura para disuadir a otros colaborares de Wikileaks. Al final la sentencia le condenó a treinta y cinco años de prisión y desestimó el más grave de ayudar al enemigo. Con los diversos beneficios penitenciarios, podría obtener la libertad condicional en ocho años tras su ingreso en la cárcel.

El fundador de Wikileaks también se ha enfrentado a una odisea legal. El 20 de agosto de 2010, dos mujeres, de veintiséis y treinta y un años, acudieron a una comisaría de Estocolmo, donde Assange residía en esa época, para solicitar que le obligasen a someterse a una prueba de detección de enfermedades de transmisión sexual, dado que había tenido relaciones con cada una de ellas por separado. Sus declaraciones fueron luego entregadas a la fiscalía, que dictó una orden de detención por acoso sexual y un término legal sueco llamado «violación leve». El 30 del mismo mes fue interrogado por la policía por el primer cargo. Por entonces ya se había desestimado el segundo. Obtuvo permiso para dejar el país y se mudó a Londres el 27 de septiembre. Dos meses después, la fiscalía sueca reactivó el caso y pidió su extradición. Esto llevó a una serie de vistas judiciales entre las autoridades británicas y la defensa del australiano, que concluyó con la aprobación de la medida. Antes de poder hacerse efectiva, el 19 de junio de 2012, el acusado entró en la embajada de Ecuador en la capital inglesa y pidió asilo político, que le fue concedido un par de meses más tarde. Para poder viajar al país andino necesita salir del edificio diplomático, lo que supondría su arresto inmediato.

Al mismo tiempo, desde 2010 Estados Unidos estaba investigándolo por sus labores al frente de Wikileaks, para lo que recurrió en primer lugar a su Ley de Espionaje del año 1917. Durante el juicio de Manning, se pusieron de manifiesto las conversaciones entre ambos, por lo que se podía entender que era cómplice. Varias agencias policiales del país están llevando a cabo investigaciones penales contra la organización y su titular y, si entre los cargos está el de colaborar con el enemigo, el mismo del que acusaron al soldado, podría arriesgarse a ser ejecutado.

Por ello, Assange se niega a salir de la embajada, al temer por su vida. Se ofreció a viajar a Suecia para responder por las acusaciones hechas allí siempre que se le garantizase que no iba a acabar en la nación norteamericana. No pudo formalizarse debido a que la legislación local prohíbe que las decisiones del gobierno puedan interferir con las judiciales. El periodista sigue en su reclusión forzada en la legación diplomática, sin una salida previsible a corto plazo.

A pesar de las controversias y las detenciones, Wikileaks tiene un considerable prestigio y ha recibido numerosos premios, como la medalla de oro de la Fundación para la Paz de Sydney, el José Couso por la Libertad de Prensa o el de los Derechos Humanos de la Asociación de Prensa de Brasil. También ha sido propuesto seis veces consecutivas para el Nobel de la Paz y una al Premio Mandela de las Naciones Unidas.

Wikileaks mantiene una buena relación o apoya a otra serie de entidades de las que ya hemos hablado en este libro. Destacan el proyecto Red TOR para la navegación anónima y el proyecto Bitcoin. Además, sin pedirlo pero también sin rechazar su ayuda, han sido defendidos por uno de los baluartes del *hacktivismo*, la pseudo-organización Anonymous.

Se entiende por *hacktivismo* el uso de herramientas informáticas para realizar ataques contra la seguridad informática de un dispositivo o entidad para reivindicar o lanzar algún tipo de mensaje social o político. El término data del año 1994, cuando fue establecido por un grupo de *hackers* radicados en Texas denominados El Culto de la Vaca Muerta (*Cult of the Dead Cow* en inglés). En el capítulo tres vimos las formas de actuar de algunos de ellos, dedicados a apoyar los conflictos tradicionales o el terrorismo. En el ocho pudimos analizar las herramientas que tienen a su disposición. Su valor reivindicativo es indudable, pero su capacidad de hacer daño de verdad es muy baja, no muy diferente a una manifestación ocasional con algunos violentos infiltrados que pudieran romper algunos cristales o mesas de negocios.

Existen formas menos violentas de activismo que no implican intrusiones, robo de datos o denegaciones de servicio. Algunas pueden ser tan efectivas como hacer copias de páginas que están censuradas en ciertos países y colgarlas en servidores y dominios que escapan al control de las autoridades, haciéndolas accesibles de nuevo. Otra forma es publicar de manera anónima información en foros, blogs, portales de vídeos o cualquier otra forma de llegar a terceros. Para ello se pueden utilizar sistemas de enmascaramiento de IP, voces generadas por ordenador o redes de anonimización. Para que el mensaje llegue a la mayor cantidad de gente posible hay técnicas que permiten que los buscadores indexen los resultados de los *hacktivistas* en las primeras posiciones o los hacen visibles mediante una técnica denominada *geo-bombardeo*. Si se añade una localización en algún lugar del mundo a un vídeo grabado en YouTube, al inspeccionar la zona en Google Earth —herramienta gratuita que permite una vista de satélite de cualquier lugar del planeta—, se observará un icono que lleva al vídeo. Al poner cientos de copias con un posicionamiento cercano, el efecto será mucho más relevante, dando la sensación de que el área es un inmenso anuncio para su visualización.

En el año 2003 un estudiante neoyorquino de quince años, Christopher Poole —de apodo *Moot*—, decidió crear un foro basado en la publicación de imágenes de forma anónima, inspirado en otros similares que ya existían en Japón. Lo llamo 4chan, que en el idioma nipón significa «cuatro hojas». La presentación de su sitio web explica que «es un foro sencillo, basado en imágenes, donde cualquiera puede publicar comentarios y compartir imágenes. Hay apartados dedicados a una variedad de intereses, desde la animación japonesa y su cultura a videojuegos, música y fotografía. Los usuarios no necesitan registrarse ni crear una cuenta antes de

participar en la comunidad». El foro creció de una forma exponencial hasta llegar a ser uno de los que más tráfico tenía en Internet. En él se crearon muchos *memes* —idea, expresada mediante gráfico, palabras, música o de cualquier otra forma, que se identifica con facilidad y se hace popular en Internet a través del boca a boca— que continúan vigentes hoy en día y que son reconocidos al instante por los más jóvenes o aquellos habituados a navegar por la Red. El más popular de los inventados allí es el conocido como *Pedobear*, el *osito pedófilo*, un plantígrado antropomorfo que actúa como depredador de niños. A menudo es usado para burlarse de aquellos que muestran tendencias pedófilas en el foro.

En 4chan se podía —y se puede— encontrar de todo. Muchos temas bordean la legalidad cuando no la atacan y allí la corrección política es una entelequia. La defensa del consumo de drogas y las fotos sugerentes, pero no pornográficas, de chicas que aún no han cumplido la mayoría de edad son habituales, como también un cierto sentimiento de pertenencia a un grupo y un interés por la seguridad informática.

Debido a que no es obligatorio registrarse, sus usuarios se llaman a sí mismos *Anon* o *Anonymous*. Su actividad reivindicativa se empezó a manifestar a finales de 2006 y principios de 2007, cuando realizaron un ataque de denegación de servicio y saturaron el teléfono con llamadas de broma al programa de radio de Hal Turner, un supremacista blanco que acabó en prisión por amenazas dos años después. Causaron la caída de su página web y, aunque demandó a 4chan, no consiguió que se aplicasen ni siquiera medidas cautelares contra ella. Otras pequeñas actividades —como descubrir la contraseña y utilizar el correo particular de Sarah Palin, candidata republicana a la vicepresidencia en 2008— se llevaron a cabo organizadas desde el foro, según sus autores para defender la libertad y a los derechos humanos, aunque sin dudar en limitar la capacidad de comunicación de terceros.

A partir de ese año empiezan a desarrollar una identidad propia. Su bandera muestra a un hombre vestido con traje cuya cabeza se ha reemplazado por un interrogante —como señal de que no tienen ningún líder ni ningún ideal— y un lema que suelen emplear en todos sus comunicados:

> *El conocimiento es libre.*
> *Somos Anónimos.*
> *Somos Legión.*
> *No perdonamos.*
> *No olvidamos.*
> *¡Espéranos!*

La máscara que creó el dibujante Alan Moore para su cómic *V de Vendetta* y que representa al revolucionario inglés Guy Fawkes se convirtió en otra de sus señas de identidad. Desde entonces ha estado en cada vídeo colgado en Internet —para así

mantener el anonimato del declarante— y en muchas de las manifestaciones a las que han acudido algunos que decían ser parte de Anonymous.

No hay que entenderlos como una organización al uso, sino más bien como una red heterogénea de personas ligeramente interconectadas que se coordinan para llevar a cabo sus acciones, que no son de todo el grupo, sino tan solo de una masa crítica de ellos, es decir, los suficientes como para ejecutarla. Pueden ser media docena para un ataque DDoS o doscientos para saturar un buzón con llamadas falsas. De hecho, una parte de quien se identifica con ellos suele oponerse a lo que va a hacer o ha hecho otro segmento. Sus miembros entran y salen con frecuencia y nunca se puede estar seguro de que uno que parece nuevo no sea un viejo conocido que ha cambiado de apodo o, al contrario, que alguien recién llegado utilice el nombre de un veterano.

Su primera acción organizados ya como Anonymous y no como parte de 4Chan —aunque fuera uno de los lugares en los que hablaban— fue contra la Iglesia de la Cienciología en 2008. Apareció en YouTube un vídeo que mostraba a Tom Cruise alabando a esa religión hasta extremos que resultaban incluso jocosos —afirmaba que solo ellos podían ayudarle si sufría un accidente de coche—. Los nombrados demandaron su retirada, porque decían que pertenecía a una grabación más larga que había sido editada para desprestigiarles. El noticiero del corazón Gawker, sin embargo, se hizo eco del vídeo y se negó a quitarlo, porque afirmaba que tenía valor informativo por sí mismo, lo que le trajo repercusiones legales y provocó la chispa que lanzó a los *anónimos* a actuar. Desde el 18 al 25 de enero *tumbaron* diferentes sitios web del credo, a pesar de los esfuerzos hechos por protegerlos de los ataques. También se infiltraron en ordenadores de las sedes y publicaron la información extraída de los mismos. Los agresores emitieron vídeos y notas de prensa en las que avisaban de que continuarían su acción para proteger la libertad de expresión. Esa fue la primera ocasión en que usaron el lema que hemos visto antes.

También llevaron a cabo acciones más *creativas*. Para muchas de ellas no hace falta tener unos conocimientos especiales, sino disponer del suficiente personal para ejecutarlas. Por ejemplo, saturaron los teléfonos de sus objetivos con llamadas falsas y enviaron multitud de faxes en negro con el propósito de hacerles gastar cartuchos de tinta. Además, como parte de su intento por menospreciar a los cienciólogos, utilizaron una técnica llamada *bomba Google* mediante la cual consiguieron que el primer resultado que apareciera al buscar «culto peligroso» fuera la página oficial de la supuesta secta. También hicieron que la página de presentación del agregador de noticias *Digg.com* —similar en cierta medida al conocido *meneame.net* español— estuviera copada de informaciones negativas sobre la cienciología.

Durante esos ataques cometieron también uno de sus primeros errores, cuando uno de los subgrupos, llamado *g00ns*, entró en el equipo informático de un hombre de cincuenta y nueve años al que creían parte de una partida de *hackers* opuestos a ellos, llamados *El Régimen*, y publicaron todos sus datos personales, incluyendo dirección, teléfono y número de la Seguridad Social para que otros los utilizaran en su contra.

Cuando se dieron cuenta del error pidieron perdón, aunque el daño ya estaba hecho.

Los más de quinientos ataques de DDoS y el resto de acciones se llevaron a cabo por unas nueve mil personas, según dijeron los organizadores en el periódico *Los Angeles Times*. Un analista de seguridad manifestó en el diario australiano *The Age* que, en cualquier caso, los atacantes serían miles. Ni siquiera para ejecutar los actos estaban coordinados, sino que cada individuo o asociación llevó a cabo las acciones que le parecieron oportunas dentro de la idea general.

El Proyecto Chanology, como se le conoció, fue un éxito, sobre todo por las repercusiones mediáticas que tuvo, que llevaron a casi dos años de manifestaciones en diferentes lugares del mundo y una amplia cobertura en prensa, dada la importancia de la religión atacada, seguida por muchos famosos y millonarios y que muchas veces ha sido sujeto de controversia sobre si entra o no en los patrones que la convertirían en una secta. Pero las acciones violentas, aunque fueran virtuales, también recibieron una crítica casi unánime, en la que se destacaron investigadores y divulgadores que se habían caracterizado por la crítica al culto.

Desde entonces, bajo el paraguas de Anonymous se han llevado a cabo muchas actividades con más o menos éxito y mayor o menor repercusión. Utilizan las técnicas que vimos en el capítulo ocho para obtener datos de lugares cuya seguridad es deficiente o perpetrar ataques de denegación de servicio con mayor o menor fortuna. En España, con motivo de la aprobación de la conocida como *Ley Sinde*, que preveía el cierre de sitios web que tuvieran enlaces a descargas de contenido protegido —películas, libros y música, sobre todo—, atacaron las páginas web del Senado y del Partido Popular. Además han realizado varias acciones en persona, siempre con la máscara de Guy Fawkes que es su seña de identidad. Así vestidos, abuchearon a la ministra González-Sinde en 2011 y a los invitados a la gala de los Premios Goya de aquel mismo año.

Una colectividad tan heterogénea no es invulnerable y, de hecho, varios de ellos han sido detenidos en diferentes lugares del mundo. El primero en ser condenado fue un estadounidense, Dmitriy Guzner, de diecinueve años, que se declaró culpable de «alteración no autorizada de un ordenador protegido», lo que le llevó a la cárcel un año y un día. Ha habido decenas más de arrestos, incluyendo siete en España, tres de ellos por los ataques a la web del Senado y los otros cuatro por las acciones de represalia por la detención de los primeros, junto a otros veintiuno en diferentes países latinoamericanos.

Algo que ha caracterizado también sus operaciones han sido los errores, meteduras de pata y daño a operaciones policiales en curso. Cuando decidió declararle la *guerra virtual* al Estado Islámico, que en buena medida se nutre, como vimos en capítulo tres, de su propaganda en la Red, causó daños muy serios a investigaciones de las diferentes policías, cuyo objetivo no es que un terrorista no tenga una cuenta de Twitter, sino detenerlo y evitar que haga más daño.

Hay que tener en cuenta que, dada la repercusión mediática de sus actos, una

equivocación puede ser desastrosa para su víctima. Con motivo de un vídeo que fue publicado en diferentes medios, en el que un hombre de mediana edad realizaba tocamientos genitales a una niña en un restaurante de la localidad de Tabasco, en México, miembros del colectivo realizaron una investigación que apuntó al abuelo de una pequeña, cuyos datos publicaron en Internet, desde su nombre a su residencia en Estados Unidos. Tres días después fue capturado el verdadero responsable, que era el padre de la verdadera víctima, vivía en México e ingresó en prisión por aquellos hechos. Meses después, en las búsquedas en Internet todavía tiene preeminencia el inocente sobre el culpable. Dadas las repercusiones sociales y morales que esos delitos acarrean, incluso la vida del abuelo está en juego. Como dice la organización belga On Focus, de protección a la infancia, con motivo de otra acción similar, «el trabajo de la policía lo debe hacer la policía y nadie más».

Algunos proveedores de servicios de Internet han considerado que las actividades de estas personas no tienen cabida en sus plataformas, por lo que Facebook, Twitter y YouTube les han eliminado las cuentas e información asociada a las mismas.

Anonymous no va a desaparecer ni dejará de actuar de un día para otro, puesto que no hay una cabeza visible que cortar ni una estrategia coordinada. Ni siquiera existe un único canal de comunicación. Es una expresión más de la diversidad de la Red y de las infinitas posibilidades que tiene, que se pueden usar de formas creativas, legales o ilegales pero, desde luego, seguirán dando que hablar, con sus luces y sus sombras.

BIBLIOGRAFÍA

1. INTERNET PROFUNDA. ¿QUÉ DEMONIOS ES ESO?

BERBELL, C. y JIMÉNEZ, L., *Los nuevos investigadores*, La Esfera de los Libros, Madrid, 2012.

CHEN, Thomas y ROBERT, Jean-Marc, *The Evolution of Viruses and Worms*, Marcel Dekker, Nueva York, 2004.

GROMOV, Gregory, «Roads and Crossroads of Internet History», *NetValley.com*, 1995.

LEINET, Barry M. *et al*., «A Brief History of the Internet», *Internet Society*, 2015.

SHORTER, K., «Plastic Payments: Trends in Credit Card Fraud», Boletín Policial del FBI, 2007.

«67 detenidos en una operación de la Europol contra la pornografía infantil en Internet», *ABC*, 6 de junio de 2006.

«Auge y caída de los piratas musicales: breve historia de la "escena MP3"», Hoja de Router en *eldiario.es*, 20 de febrero de 2015.

«Detenido en Gipuzkoa por poner fotos de los amigos de sus hijos en un foro pedófilo», *Diario Vasco*, 17 de mayo de 2009.

«Detenido por piratear la WiFi», *El Mundo*, 26 de noviembre de 2013.

«Detenido un pedófilo que infectaba ordenadores y grababa a sus vecinos en Zaragoza», *Heraldo de Aragón*, 2 de mayo de 2013.

«eDonkey Backer Agrees to $30 Million Settlement», *The New Yort Times*, 13 de septiembre de 2006.

«EEUU impone la primera multa por descargar ilegalmente música de Internet», *Expansión*, 5 de octubre de 2007.

«La Ñ, clave en el caso Kova, se detectó en Canadá», *ABC*, 29 de mayo de 2005.

«La policía detiene a 21 personas por fraude y estafa por internet», *El Periódico de Extremadura*, 5 de febrero de 2005.

«La red TOR sufre un ataque que puede haber dejado a sus usuarios al descubierto», Diario Turing de *eldiario.es*, 1 de agosto de 2014.

«Nanysex pasó la vida huyendo de su rastro», *El País*, 22 de junio de 2008.

«Razorback2 killed», *The Inquirer*, 22 de febrero de 2006.

2. EL HOGAR DEL PEDERASTA

BRONGERSMA, E., «Schutzalter 12 Jahre?-Sex mit Kindern in der Niederländischen Gesetzgebung», en LEOPARDI, A., *Der padosexuelle Komplex*, Foerster, Berlín, 1988.

VICKERS, G., *Chasing Lolita: How Popular Culture Corrupted Nabokov's Little Girl*

All Over Again, Chicago Review Press, 2008.
«29 años de cárcel para el ciberacosador millonario»[5], blog Luz de Luna de *Telecinco.es*, 26 de noviembre de 2013.
«Ad Van der Berg, fundador del extinto partido pro pedofilia en Holanda: "Yo nunca he buscado niños, los niños vienen a mí"», *The Clinic*, 6 de enero de 2014.
«Canada's Biggest Child Porn Case ends With Conviction on 15 Charges», *The Star*, 12 de mayo de 2015.
«Colorado Middle School Teacher, 24, "Had Long-Term Sexual Relationship with SIXTH GRADE Student and Gave Him Marijuana"», *The Daily Mail*, 9 de mayo de 2015.
«Confirman la pena de 17 años para un padre que abusó de sus hijos», *Última Hora*, 15 de abril de 2013.
«Detenido en Lima un pederasta con más de 500 víctimas menores de edad». *El Periódico*, 30 de noviembre de 2013.
«El ciberacosador de Chipiona estará 11 años en la cárcel por acosar a 67 jóvenes», *La Voz Digital*, 18 de mayo de 2012.
«El ciberacosador de Chipiona obligó a una de sus víctimas a enviarle vídeos pornográficos», *Canal Sur Noticias*, 12 de marzo de 2012.
«El sexo con animales dejará de ser impune», *ABC*, 16 de enero de 2015.
«Global Raids Shut *boylover.net*, Arrest 184 Men, Rescue 230 kids», *Ars Technica*, 17 de marzo de 2011.
«La pedófila que quería adoptar un niño», *Informativos Telecinco*, 7 de abril de 2011.
«Police Shut Ukraine Model Agency in Porn Crackdown», Agencia Reuters, 28 de julio de 2004.
«Seis años de cárcel para el pederasta valenciano apresado en Guatemala», *El Mercantil Valenciano*, 23 de junio de 2010.
«Suicídate. Te será más fácil», *Público*, 22 de octubre de 2009.
«The FBI's Largest Ever Blow to Child Porn and the Deep Web, and Its Possible Ripple Effects», *Extreme Tech*, 5 de agosto de 2013.
«Un pederasta con piel de cordero», *Las Provincias*, 11 de febrero de 2007.
«Victim Identification», Área de Delitos contra Menores de la página web oficial de Interpol, consultada el 29 de agosto de 2016.
«Viola a cuatro hijos de tres a seis años y los "ofrece" en la Red», *La Razón*, 14 de mayo de 2011.

3. LA GUERRA NO CONTEMPLADA

EHRENBERG, Rachel, «Scientists surf Web's dark Side: Mathematical Tools Collect Information on Extremists», *Science News*, 10 de marzo de 2012.
MAKOVSKY[6], David, «The Silent Strike», *The New Yorker*, 17 de septiembre de

2012.
NYE, Joseph S., «El futuro del poder», *Project Syndicate*, 8 de octubre de 2010.
PAGE, Lewis, «Israeli Sky-Hack Switched off Syrian Radars Countrywide», *The Register*, 22 de noviembre de 2007.
REED, Thomas, *At the Abyss: An Insider's History of the Cold War*, Presidio Press, 2005.
REGUERA SÁNCHEZ, Jesús, *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario*, Grupo de Estudios en Seguridad Internacional, 2015.
SANGER, David, *Confront and Conceal: Obama's Secret Wars and Surprising Use of Military Power*, Broadway Books, 2012.
SCHMITT, Michael, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, US Naval War College, 2009.
TORRES SORIANO, Manuel, «¿Es el yihadismo una ciberamenaza?», *Revista de Occidente*, n.º 406, marzo de 2015.
«*Charlie Hebdo*: Now Islamic Hackers Launch Cyber-Jihad Against France in Support of Terror Attacks», *The Daily Mirror*, 12 de enero de 2015.
«Cuartel general antihackers», *XLSemanal*, 19 de julio de 2015.
«Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?», Institute for Science and International Security, 2010.
«El navegante», *El Mundo*, 16 de abril de 1999.
«Electronic Weapons: Smiting Syria With Suter», *The Strategy Page*, 6 de octubre de 2007.
«Espías, asesinatos y desertores», *El País*, 15 de enero de 2012.
«Hackeo islamista masivo de páginas de ayuntamientos de Navarra». *ABC*, 20 de enero de 2015.
«Iran Hangs "Mossad spy" Majid Jamali Fashi for Killing Scientist», *The Independent*[7], 16 de mayo de 2012.
«Myth: Israel's Strike on Iraqi Reactor Hindered Iraqi Nukes», Institute for Public Accuracy[8], 16 de marzo de 2006.
«Nadie está a salvo de esta ciberguerra», *El País*, 10 de diciembre de 2010.
«North Korea doubles its cyber warfare team to 6,000 troops», *Daily Telegraph*, 7 de enero de 2015.
«Update on Sony Investigation», nota de prensa, Federal Bureau of Investigation, 19 de diciembre de 2014.

4. LA MUERTE RETRANSMITIDA

SANDERS, Ed., *The Family: The Story of Charles Manson's Dune Buggy Attack*

Battalion, Dutton, Boston, 1971.
«Australian Behind "Daisy" Sex Videos Charged», ABS CBS News, 6 de marzo de 2015.
«Comienza en Alemania el juicio contra un hombre acusado de canibalismo», *El País*, 3 de diciembre de 2003.
«Del Olmo clausura una web norteamericana con imágenes crudas del 11-M», *La Vanguardia*, 25 de octubre de 2004.
«Dutch Cops, NBI Save Kids From PH Porn Hell», *The Inquirer*, 1 de marzo de 2015.
«Peter Gerard Scully Made Philippines Children dig Own Grave: Victims», *The Age,* 1 de marzo de 2015.
«Remy Couture, artista de efectos especiales de Quebec, fue declarado inocente en caso sobre obscenidad», *Noticias Montreal*, 23 de diciembre de 2012.
«Shock and Gore», *Financial Times*, 13 de enero de 2006.
«Tres detenidos por difundir en Internet las fotografías de los cadáveres del 11-M»[9], *ABC*, 30 de octubre de 2004.
«Web Child Fight Videos Criticised», *BBC News*, 29 de julio de 2007.

5. LOS NEGOCIOS ILEGALES

BEARMAN, Joshuah, «The Rise and Fall of *Silk Road*», *Wired*, mayo de 2015.
«¿Quién está detrás de los nuevos 60 000 seguidores falsos de Mariano Rajoy en Twitter?», *20 minutos*, 5 de septiembre de 2014.
«Cae una red de "cibernarcos" que vendía cocaína en Internet», *20 minutos*, 9 de agosto de 2014.
«Cuatro detenidos por la falsificación de títulos, que se vendían en internet»[10], *La Verdad de Murcia*, 26 de enero de 2010.
«Desarticulan una red de pederastas que grababa y distribuía los abusos que cometían sobre menores», *El Mundo*, 13 de febrero de 2005.
«Pablo Iglesias y Miguel Ángel Revilla, los más populares en las redes sociales», *La Voz Libre*, 16 de diciembre de 2015.
«Secret Website Harboured Drugs Smorgasbord, Court Hears», *The Age*, 31 de enero de 2013.
«Variety Jones, Alleged *Silk Road* Mentor, Arrested in Thailand», *Wired*, 4 de diciembre de 2015.
Comunicados de prensa del Departamento de Justicia de los Estados Unidos.
Notas de prensa del Ministerio del Interior de España.

6. LOS PROFESIONALES DEL ROBO

«28 encarcelados por el timo de la lotería falsa» *El País*, 17 de abril de 2008.
«49 detenidos por estafar a clientes de empresas mediante "phishing"», *El Periódico*, 10 de junio de 2015.
«Detenido un grupo criminal por 43 delitos de estafa con tarjetas de crédito falsas», *El Mundo*, 28 de diciembre de 2015.
«El cibercrimen financiero de habla rusa: *modus operandi*», *Securelist.lat*, 19 de noviembre de 2015.
«First Case of "Drive-by Pharming" Identified in the Wild», *Network World*, 22 de enero de 2008.
«La estafa del "carding": usar tarjetas bancarias extranjeras para comprar en España», *ABC*, 18 de abril de 2015.
«Shadowy Russian Firm Seen as Conduit for Cybercrime», *The Washington Post*, 13 de octubre de 2007.
Circular 2/2011 de la Fiscalía General del Estado.
Notas de prensa de Interpol.
Notas de prensa del FBI.

7. EL DINERO QUE EXISTE Y NO EXISTE A LA VEZ

LEHDONVIRTA, Vili y CASTRONOVA, Edward, *Virtual Economies, Design and Analysis*, MIT Press, Cambridge, 2014.
LUDLOW, Peter, *Alphabilleherald.com*.
MANJOO, FARHAD, «Raking muck in *The Sims Online*», *Salon*, 12 de diciembre de 2003.
NAKAMOTO, Satoshi, «Bitcoin: A Peer-to-Peer Electronic Cash System», *www.bitcoin.org*.
STEPHENSON, Neal, *Criptonomicón*, Editorial Avon, 1999.
WILSON, Daniel y ZENIL, Hector, *On the Complexity and Behaviour of Cryptocurrencies Compared to Other Markets*, Cornell University Library, Nueva York, 2014.
«China Used Prisoners in Lucrative Internet Gaming Work», *The Guardian*, 25 de mayo de 2011.
«Could Linden Dollars Become Real Money?», *Hypegrid Business*, 5 de abril de 2013.
«The Coin Prince: Inside Bitcoin's First big Money-Laundering Scandal», *The Verge*, 4 de febrero de 2014.
«The European Union May Prohibit Cryptocurrency Transactions from Some Countries», *Forklog*, 14 de febrero de 2016.
«The Missing MtGox Bitcoins», *Wizsec*, 19 de abril de 2015.

«Trading Site Failure Stirs Ire and Hope for Bitcoin», *New York Times*, 25 de febrero de 2014.
Notas de prensa del IRS (Internal Revenue System) del 25 de marzo de 2014.
Resolución 044/2014 de 6 de mayo del Banco Central de Bolivia.

8. *HACKERS*: EL ARTE DE LO POSIBLE

CORRONS, Luis, «Identificadas aplicaciones de Google Play que suscriben a SMS premium sin permiso», Panda Security, blog personal, 12 de febrero de 2014.
«“Melissa” Creator Gets 2nd Jail Term», *CBS News*, 1 de mayo de 2002.
«Anonymous “hackea” la web de la mutua de la Policía Nacional», *El País*, 1 de junio de 2016.
«Apartado de sus funciones el maestro de Figueres acusado de pedofilia», *El Mundo*, 25 de marzo de 2010.
«Cinco curiosidades sobre el virus de la policía», Oficina de Seguridad del Internauta, 12 de septiembre de 2014.
«Condenado a seis años de cárcel por hacerse pasar por la policía con un virus informático», *El Mundo*, 29 de febrero de 2016.
«Desarticulada la banda que creó el virus informático de la policía», *El Periódico*, 27 de septiembre de 2013.
«Detenido el creador de una falsa aplicación para espiar conversaciones de WhatsApp», *ABC*, 22 de julio de 2013.
«Detenido en Córdoba el “hacker de las actrices”», *Público*, 12 de marzo de 2016.
«Detenido in fraganti un pedófilo cuando intercambiaba imágenes de pornografía infantil en un locutorio», *El Mundo*, 15 de febrero de 2015.
«Detenido un exjefe de Intereconomía por atacar la web de Prnoticias», *El País*, 14 de diciembre de 2014.
«Lafuente, el *hacker* que contrató a un pirata libanés por orden de Julio y Julen Ariza»[11], *PRNoticias.com*, 21 de diciembre 2014.
«Taking Down Botnets: Microsoft and the Rustock Botnet», TechNet, blog oficial de Microsoft, 17 de marzo de 2011.
«Un pedófilo espiaba a más de 100 vecinos a través de la red WiFi con un sofisticado software», *20 minutos*, 2 de mayo de 2013.
«Un virus para Android suscribe a las víctimas en servicios premium», *Cinco Días*, 8 de noviembre de 2012.
«XCodeGhost: Una cadena de estupideces infecta aplicaciones populares en iOS», *Hipertextual*, 19 de septiembre de 2015.
Enciclopedia de virus y amenazas de *F-Scure.com*.
Ley de Enjuiciamiento Criminal.

9. LA VOZ DE LOS NECIOS

CANTÓ, Antonio, *La pizarra de Yuri. Historias de ciencia al calor del fuego*, Silente Académica, Guadalajara, 2011.

FERRER BENIMELI, José Antonio, «Franco contra la Masonería», *Historia 16*, 1977.

GÁMEZ, Luis Alfonso, *El peligro de creer*, Léeme Editores, Alcalá de Henares, 2015.

LÓPEZ ITURRIAGA, Juan Manuel, «No te creas el vídeo de la manzana», blog «El Comidista», *El País*, 21 de enero de 2015.

SALUSTIO CRISPO, Cayo, *La conjuración de Catilina; Guerra de Jugurta*, Akal, Madrid, 2001.

«La policía detiene a cuatro jóvenes por difundir falsas amenazas terroristas», *El País*, 19 de noviembre de 2015.

«Los dos acusados de ayudar a suicidarse a una mujer aceptan dos años de prisión», *La Nueva España*, 25 de mayo de 2015.

«Los padres del niño con difteria, destrozados, se sienten engañados por los antivacunas», *La Vanguardia*, 7 de junio de 2015.

«Muere el niño de seis años enfermo de difteria en Olot», *El País*, 27 de junio de 2015.

«Retraction-Ileal-Lymphoid-Nodular Hyperplasia, Non-Specific Colitis, and Pervasive Developmental Disorder in Children», *The Lancet*, febrero de 2010.

«Revealed: MMR Research Scandal», *The Sunday Times*, 22 de febrero de 2004.

«The Conspiracy Theory Detector», *Scientific American*, 1 de diciembre de 2010.

«Wakefield's Article Linking MMR Vaccine and Autism was Fraudulent», *The BMJ*, 6 de enero de 2011.

10. LOS GOBIERNOS DEL SILENCIO

GABOR, Assaf y RISHÓN, Makor, «La Primavera Árabe. ¿Hacia una guerra civil islámica?», *Comunidades*, 16 de agosto de 2016.

«Anonymous: la revolución que ríe bajo la máscara», *La Vanguardia*, 27 de marzo de 2016.

«China Detains Teacher for Earthquake Photos», *The Guardian*, 31 de julio de 2008.

«Detenidos cuatro miembros de Anonymous en España», *20 minutos*, 28 de febrero de 2012.

«El "español" que inspiró el movimiento Anonymous», *El Mundo*, 6 de noviembre de 2015.

«El papel de Internet y de las redes sociales en las revueltas árabes: una alternativa a la censura de la prensa oficial», *Comunicar*, n.º41, vol. 21, 2013.

«Encarcelan formalmente al presunto padre pederasta captado en vídeo en Tabasco, México», Univisión, 15 de abril de 2016.

«Freedom On The Net 2015», informe de la ONG Freedom House, octubre de 2015.
«Garzón defenderá al fundador de *Wikileaks*, Julian Assange», *El País*, 25 de julio de 2012.
«Google Search Results For Tiananmen Square: UK Vs. China (PICTURE)», *The Huffington Post*, 25 de mayo de 2011.
«Internet en Cuba: lenta y cara, pero cada vez más masiva»[12], *Infobae*, 7 de mayo de 2016.
«Julian Assange cumple tres años recluido en la embajada de Ecuador en Londres», *20 minutos*, 19 de junio de 2015.
«La extraña experiencia de navegar internet en Corea del Norte», *BBC Mundo*, 12 de diciembre de 2012.
«Los detenidos de Anonymous se enfrentan a una pena de uno a tres años de cárcel», Agencia Europa Press, 10 de junio de 2011.
«Sólo uno de los seis países de la Primavera Árabe es democrático», *El Mundo*, 15 de marzo de 2016.
«The Alibaba Phenomenon», *The Economist*, 23 de marzo de 2013.
«The Deadly Beating that Sparked Egypt Revolution», Noticias CBS, 2 de febrero de 2011.
«Túnez según los cables diplomáticos filtrados por *Wikileaks*», *El País*, 14 de enero de 2011.
«Tweeting Tyrants Out of Tunisia: Global Internet at Its Best», *Wired*, 14 de enero de 2011.
«WikiLeaks Exposed Sensitive Data on Hundreds of Innocent People, Including Rape Victims», *The Verge*, 23 de agosto de 2016.
Informe sobre Túnez de la página del proyecto Red Abierta (*www.opnennet.net*), 7 de agosto de 2009.
www.wikileaks.org



Eduardo Casas Herrer, nacido en Zaragoza, es técnico superior en informática y miembro del Cuerpo Nacional de Policía desde 2004 en la Unidad de Investigación Tecnológica. Está especializado en la lucha contra la explotación sexual de menores, por la que ha sido condecorado en varias ocasiones. Es miembro permanente del Grupo de Expertos en Identificación de Víctimas de Interpol, que se encarga de la localización de niños explotados sexualmente en Internet y de sus agresores.

Profesor honorario de la Universidad Autónoma de Madrid, donde imparte lecciones de posgrado para el Instituto de Ciencias Forenses y de la Seguridad, y de la Universidad Complutense de Madrid, para la que da clase en el tercer curso de Criminología, da charlas y conferencias en diversas entidades, desde colegios a diputaciones provinciales.

Es autor de dos novelas, Cristal traslúcido y El juez de Sueca, y ha ganado más de veinte concursos de narrativa corta.

Notas

[1] Nombre ficticio. <<

[2] Nombre cambiado para preservar la identidad de la víctima. <<

[3] https://en.wikipedia.org/wiki/Kristinn_Hrafnsson <<

[4] https://en.wikipedia.org/wiki/Sarah_Harrison_(journalist) <<

[5] http://www.telecinco.es/blogs/luzdeluna/Manuel_Joaquin_Blanco_Garcia-ciberacosador-Angel_Moya-Malena_Guerra-Operacion_TAMO_6_1706865004.html
<<

[6] http://www.newyorker.com/contributors/david-makovsky <<

[7] http://www.independent.co.uk/biography/donald-macintyre <<

[8] https://es.wikipedia.org/w/index.php?title=Institute_for_Public_Accuracy&action=edit&redlink=1 <<

[9] http://www.abc.es/hemeroteca/historico-30-10-2004/abc/Ultima/tres-detenidos-por-difundir-en-internet-las-fotografias-de-los-cadaveres-del-11-m_963177872838.html <<

[10] http://www.laverdad.es/agencias/20100302/mas-actualidad/espana/0 <<

[11] http://prnoticias.com/internet-y-redes-socialespr/362-pr-no-se-calla-1/20137070-prnoticas-hacker-julio-ariza <<

[12] http://www.infobae.com/2016/05/07/1809387-internet-cuba-lenta-y-cara-pero-cada-vez-mas-masiva <<